DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS CON SNORT PARA LA COMPAÑÍA SILVERIT SAS.

ANDRÉS FELIPE RODRÍGUEZ GUTIÉRREZ

Proyecto de grado

Ing. Cesar Rodríguez

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2016

Nota de aceptación

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del Jurado

_____
Firma del Jurado

CONTENIDO

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

INTRODUCCIÓN

La tecnología se ha vuelto parte fundamental en la vida de los seres humanos, a diario se hace uso de esta para trabajar, jugar, estudiar y muchas cosas más.

Actualmente existen aproximadamente 3.0 billones de usuarios conectados a internet, 3.3 billones de smartphones conectados a internet, 16.6 billones de ip's, 72.4 de exabytes de tráfico en la red y se estima que para el 2019 existan cerca de 4.0 billones de usuarios conectados a internet, 5.9 billones de smartphones conectados a internet, 24.4 billones de ip's y 168.4 exabytes de tráfico en la red.

Todas las compañías desde las pequeñas empresas hasta las grandes multinacionales han hecho de la tecnología un aliado estratégico para la optimización de sus procesos. Cada día buscan innovar e implementar nuevas tecnologías como computación en la nube, páginas de internet, portales transaccionales, entre otros.

En muchas ocasiones estas compañías no tienen en cuenta la seguridad de estos sistemas de información ya sea por falta de conocimiento, personal no capacitado, falta de presupuesto o tal vez no se le da la importancia necesaria.

Según el periódico la vanguardia[1] en un artículo publicado el 11 de marzo de 2014 el 98% de las empresas colombianas son víctimas de ataques informáticos, a pesar de que el gobierno ha venido trabajando en leyes para castigar este tipo de delitos como la ley 1273 de 2009, la ciberdelincuencia ha venido en aumento, lo cual hace pensar que se debe estar listo y preparado para proteger el principal activo de su compañía, la información.

1. JUSTIFICACIÓN

[1] 98% de empresas colombiana son víctimas de ataques informáticos. En: La vanguardia. Bucaramanga. 11, marzo, 2014. [online] Disponible en internet, agosto 2016 <URL: http://www.vanguardia.com/actualidad/colombia/250540-98-de-empresas-colombianas-son-victimas-de-ataques-informaticos >

Este proyecto se llevará a cabo en SILVERIT SAS una compañía que lleva un año en el mercado, se desenvuelven en el sector tecnológico, ofreciendo servicios de consultoría en seguridad informática, seguridad de la información, desarrollo de software e infraestructura.

SilverIT como pionera en seguridad informática sabe que la información es un activo invaluable tanto para la compañía como para sus clientes y que para mantener la integridad, disponibilidad y confidencialidad de sus sistemas de información debe implementar controles físicos, lógicos y tecnológicos. Un IDS es una herramienta muy útil para detectar irregularidades en el tráfico de red, tiene la capacidad de generar alarmas las cuales permitirán actuar rápidamente y a su vez llevar estadísticas de los incidentes presentados con el fin de evaluar los controles existentes y si es necesario implementar nuevos controles de forma que se conviertan en un plan de mejora continua sobre el sistema de seguridad informática de la compañía.

Por último, cabe resaltar el apoyo que se quiere brindar a las empresas en el tema de seguridad informática, aunque SilverIT es una empresa dedicada a prestar este tipo de servicios no cuenta con un sistema de detección de intrusos que hoy en día forma parte esencial de un sistema de seguridad. Así mismo, existen muchas empresas que desconocen acerca de la importancia de contar con un esquema de seguridad informática.

2. DEFINICIÓN DEL PROBLEMA

Con el avance rápido de la tecnología esta dejo de ser un lujo para convertirse en una necesidad para las personas y las compañías, muchos de los procesos que antes se hacían de forma manual o presencial se han venido automatizando con el pasar del tiempo dejando atrás largas filas, minimizando la pérdida de tiempo, evitando errores o inexactitud de los seres humanos.

De la mano del avance tecnológico aparecieron nuevas figuras como los hackers, lammers y crackers, caracterizados por ingresar a sistemas informáticos sin un permiso previo, con el fin de hacerle frente a estas figuras se ha venido innovando en dispositivos de seguridad que sean capaces de contener nuevos ataques informáticos.

SilverIT S.A.S cuenta con varios controles de seguridad perimetral que pueden contener algunos ataques, pero a nivel de red área local los controles no son suficientes para detectar ataques informáticos, dichos ataques pueden provenir de insiders o cualquier persona que esté en la red, exponiendo a SilverIT a la perdida de disponibilidad, integridad y confidencialidad de su información y servicios.

¿Cómo se pueden detectar ataques informáticos en la red de área local de SilverIT?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un sistema de detección de intrusos con SNORT en SILVERIT SAS, este se llevará a cabo mediante una evaluación de la infraestructura de la compañía la cual permitirá conocer datos exactos para la realización del diseño del sistema de detección de intrusos. Este IDS les permitirá detectar anomalías y patrones en el tráfico de la red de área local, convirtiéndose en una herramienta de gran utilidad para el administrador de seguridad informática ya que podrá generar alertas tempranas y así contrarrestar ataques informáticos.

3.2 OBJETIVOS ESPECÍFICOS

- Recolectar información acerca del estado actual de la red e infraestructura de la compañía, esta recolección de información se realizará de la mano del área de IT.
- Analizar la información recolectada para realizar un diseño coherente con la red e infraestructura actual.
- Generar varias alternativas de solución.
- Establecer espacios de interacción con el personal de SilverIT S.A.S para debatir avances e inquietudes del proyecto.

4. MARCO TEÓRICO

4.1 HISTORIA

La historia de los detectores de intrusos se remonta a 1980. Debido al crecimiento de la tecnología e incremento en el número de los ordenadores, los logs y eventos fueron creciendo en forma exponencial por lo cual eran más difíciles de revisar y controlar, la fuerzas armadas estadounidenses dándose cuenta de este problema decidieron tomar acciones, En 1980 James P. Anderson fue el primero en documentar la necesidad mencionada, su estudio fue llamado inicialmente como "Monitor de referencias" el cual proponía un sistema de clasificación entre ataques internos y externos[2].

4.2 QUE ES UN SISTEMA DE DETECCIÓN DE INTRUSOS

Un sistema de detección de intrusos funciona como una alarma antirrobo que monitorea el lugar si se compara con el mundo físico, en el mundo de la seguridad informática la forma más simple de definir un IDS es como una herramienta especializada capaz de interpretar el contenido de los archivos de registro de routers, firewalls, servidores y otros dispositivos de red. Por otra parte los IDS hacen uso de unas firmas que les permite detectar ataques informáticos por medio de la comparación entre las mismas permitiendo que este pueda generar alarmas, dejar un registro en sus logs e informar al administrador de red o seguridad y asi tomar las acciones correspondientes, en caso de que el IDS sea utilizado para monitorear la red este funcionaria de forma similar a un antivirus pues lee los paquetes de red, los descompone y los vuelve a armar analizando su contenido por medio de las firmas que este contiene como se mencionó anteriormente[3].

4.3 FUNCIONAMIENTO DETECTOR DE INTRUSOS

El funcionamiento de un IDS se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como lo puede ser el escaneo de puertos, paquetes malformados, etc. El IDS no sólo analiza qué tipo de tráfico se genera, sino que también revisa el contenido y su comportamiento. Normalmente esta herramienta se integra con un firewall. El detector de intrusos es incapaz de detener los ataques por sí solo, excepto los que trabajan conjuntamente en un

[2] Gonzales Gómez Diego. Sistemas de Detección de Intrusiones. Barcelona. 2003. P. 17-18.

[3] Beale, Jay, et al. Snort 2.0 Instrusion Detection, Rockland, MA, Syngress Publishing, 2003. 2-3 p.

dispositivo de puerta de enlace con funcionalidad de firewall, convirtiéndose en una herramienta muy poderosa ya que se une la inteligencia del IDS y el poder de bloqueo del firewall, al ser el punto donde forzosamente deben pasar los paquetes y pueden ser bloqueados antes de penetrar en la red. Los IDS suelen disponer de una base de datos de “firmas” de ataques conocidos[4].

4.3.1 Detección basada en firmas: Una firma es un patrón que corresponde a una amenaza conocida. La Detección basada en firmas es el proceso de comparación de firmas contra los eventos observados para identificar posibles eventos, por ejemplo:

- Un intento de telnet con un nombre de usuario "root", que es una violación de la política de seguridad de una organización.
- Un correo con asunto “¡Fotos gratis!" y un nombre de archivo adjunto de "freepics.exe", que son características de una forma conocida de malware.

La detección basada en firmas es muy eficaz en la detección de amenazas que ya son conocidas, pero cuando estas son desconocidas, por ejemplo, las amenazas zero day este tipo de detección sería totalmente ineficaz ya que hasta que no se cree la firma será imposible detectar el ataque, también se deben tener en cuenta las técnicas de evasión que se usan para cambiar el patrón y que los ataques no sean detectados.

4.3.2 Detección basada en anomalías: Es el proceso de comparación de definiciones de actividades normales donde se pueden observar desviaciones significativas, utilizando este tipo de detección se tienen perfiles como usuarios, host, conexiones de red o aplicaciones que permitan hacer un seguimiento y determinar características de dichas actividades.

Por ejemplo, un usuario que diariamente consume el 2% del ancho de banda del canal de internet, de un día para otro empezó a consumir el 10%, bajo un método estadístico el IDS identificara que la actividad web comprende mucho más ancho de banda de lo esperado y alertará al administrador de la anomalía. El principal beneficio de los métodos de detección basados en anomalías es que pueden ser muy eficaces en la detección de amenazas previamente desconocidos[5].

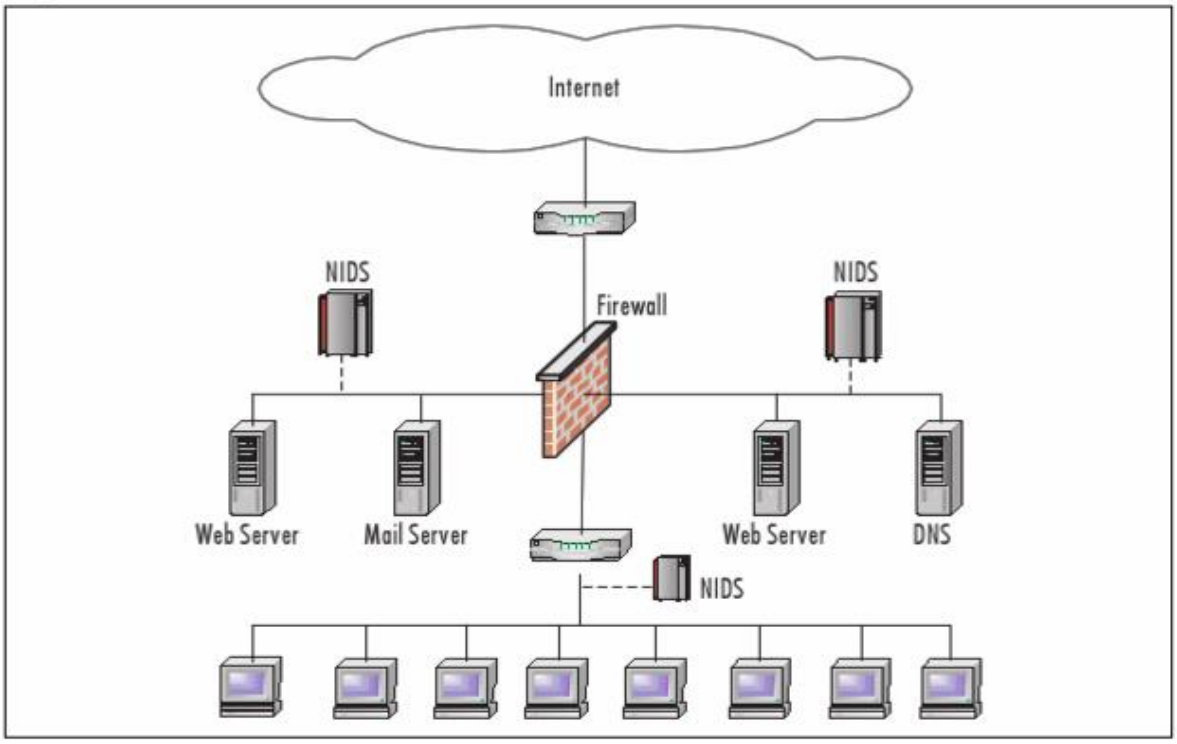
4.4 TIPOS DE IDS

[4] Tsai, Jeffrey J. P. Intrusion Detection: A Machine Learning Approach. River Edge, NJ, USA: World Scientific & Imperial College Press, 2011. ProQuest ebrary. Web. 24 September 2015. Pág. 41

[5] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Guide to intrusión detection and prevention systems (IDPS). SP 800-94, Gaithersburg 2007 2-4 p.

4.4.1 Detector intrusos de red: El NIDS es aquel que puede observar todo el tráfico que pasa por la red, para mejorar su eficacia se monitorea un segmento de red completo. Normalmente, cuenta con dos tarjetas de red una de administración y una que funciona en modo promiscuo. El NIDS debe funcionar en modo promiscuo para monitorear el tráfico de red no destinado a su propia dirección MAC. En este modo, el NIDS puede espiar todas las comunicaciones en el segmento de red, sin embargo, con los cambios en la legislación colombiana es una responsabilidad que se debe tener en cuenta. En la Figura 1, se observa una red con tres NIDS que se han colocado en los segmentos de red estratégicos y puede controlar el tráfico de la red para los dispositivos que pertenecen a cada segmento.

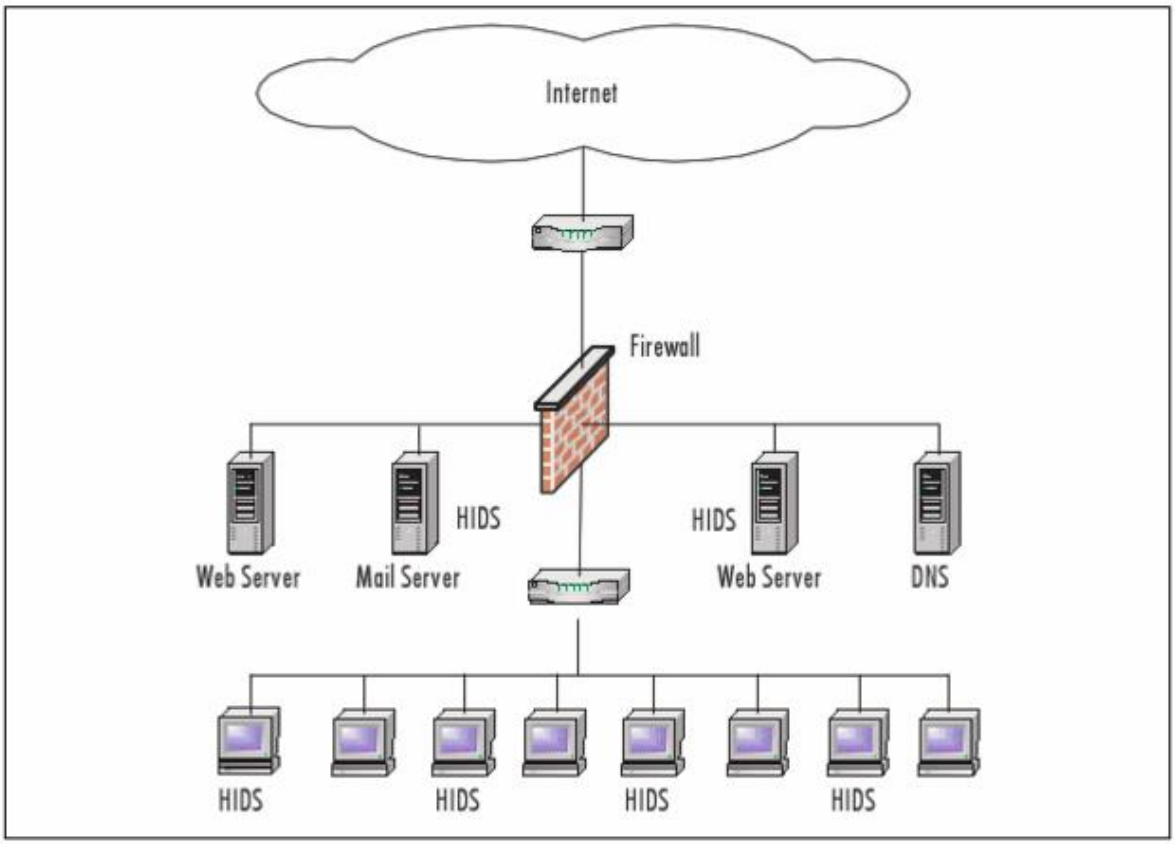
Figura 1. Ubicación NIDS



Fuente: Beale, Jay, et al. Snort 2.0 Instrusion Detection, Rockland, MA, Syngress Publishing, 2003.

4.4.2 IDS basado en host: Los HIDS funcionan localmente en los equipos de los usuarios finales como se ve en la figura 2. Los HIDS difieren de los NIDS en que la tarjeta de red del equipo no debe funcionar en modo promiscuo ya que el HIDS trabaja localmente, por ejemplo, este se fija en las anomalías de ficheros importantes para el sistema operativo como lo puede ser el archivo host, este puede ser editado con el fin de realizar un ataque de envenenamiento de DNS[6].

Figura 2. Ejemplo HIDS



Fuente: Beale, Jay, et al. Snort 2.0 Instrusion Detection, Rockland, MA, Syngress Publishing, 2003.

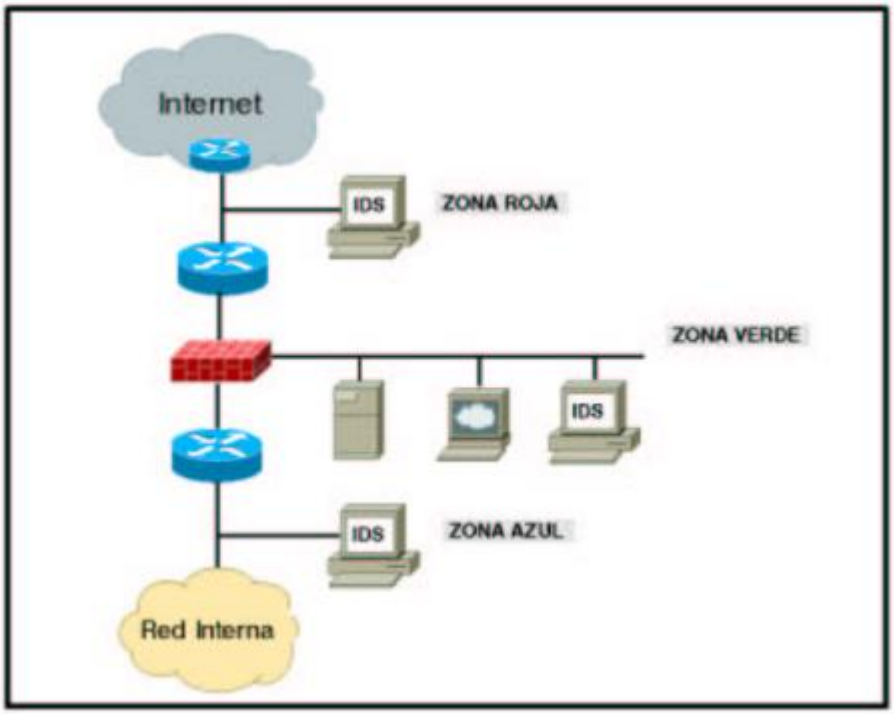
[6] Beale, Jay, et al. Snort 2.0 Instrusion Detection, Rockland, MA, Syngress Publishing, 2003. 5-6 p.

4.5 ¿DÓNDE COLOCAR UN IDS?

La decisión de donde localizar el IDS es la primera a tener en cuenta una vez que se está dispuesto a instalar un IDS. De esta decisión dependerá tanto el equipo que se use, como el software IDS o la base de datos.

4.5.1 Ubicación IDS: Existen principalmente tres zonas en las que se puede poner un sensor, tal y como lo muestra la figura 3.

Figura 3. Ubicación IDS



Fuente: Mira Alfaro José Emilio. Implantación de un sistema de detección de intrusos en la universidad de valencia. Valencia, España. Universidad de valencia. Facultad de informática. 23 p.

Las características que presenta cada una de estas zonas son:

- **Zona roja:** Esta es de alto riesgo. En esta zona el IDS debe ser configurado para ser poco sensible, puesto que pueden existir muchos falsos positivos.

- **Zona verde:** En esta zona el IDS debería tener un poco más de sensibilidad ya que el firewall realiza un primer filtro por ende deben existir menos falsos positivos.
- **Zona azul:** Esta es la zona de confianza. El IDS debe tener una mayor sensibilidad y cualquier tipo de alarma que se genere debe ser inmediatamente revisada ya que en esta zona los falsos positivos deben ser muy pocos[7].

4.6 LIMITACIONES DE LOS NIDS

Los NIDS no son capaces de reconstruir exactamente lo que han monitoreado, los IDS basados en firmas realizan un análisis pasivo del protocolo, examinando que los paquetes transmitidos hagan match con sus firmas, adicionalmente algunos de los ataques que se realizan van con los paquetes fragmentados o solapados en caso que el IDS no este configurado correctamente y con la sensibilidad adecuada no generará ningún tipo de alarma.

Existen otros tipos de ataques como los ataques con firmas polifórmicas que van mutando o simplemente el código es el mismo pero escrito de otra forma, algo muy similar a lo que sucede con los antivirus ya que no hacen un análisis heurístico de los paquetes (por ejemplo, un exploit con un shellcode bien conocido) puede cambiar el juego de instrucciones en ensamblador con una funcionalidad idéntica, pero que generará una firma distinta y por lo tanto no será detectado por el IDS.

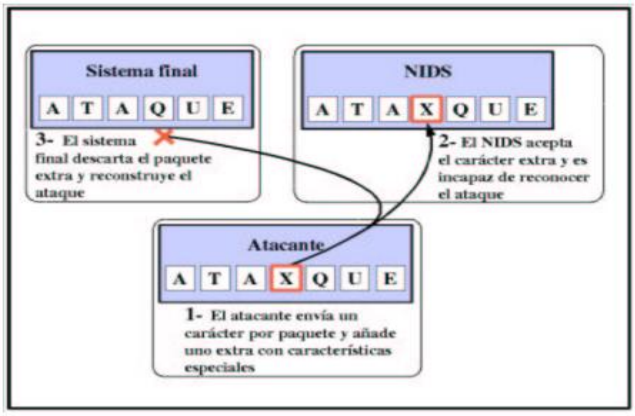
Otros tipos de ataques se generan directamente hacia el IDS, como por ejemplo los ataques de denegación de servicio, si este no está bien protegido puede quedar fuera de servicio lo cual dejaría indefensa la red ya que los ataques nunca serian detectados.

Sin embargo, los ataques para evadir los IDS que más estragos causan son los de ’inserción’ y ’evasión’, que se mencionan a continuación.

4.6.1 Inserción: El ataque de inserción se basa en que un IDS puede aceptar paquetes que luego un sistema final va a rechazar. La figura 4 da un ejemplo del ataque.

[7] Mira Alfaro José Emilio. Implantación de un sistema de detección de intrusos en la universidad de valencia. Valencia, España. Universidad de valencia. Facultad de informática. 23 p.

Figura 4. Ataque de inserción

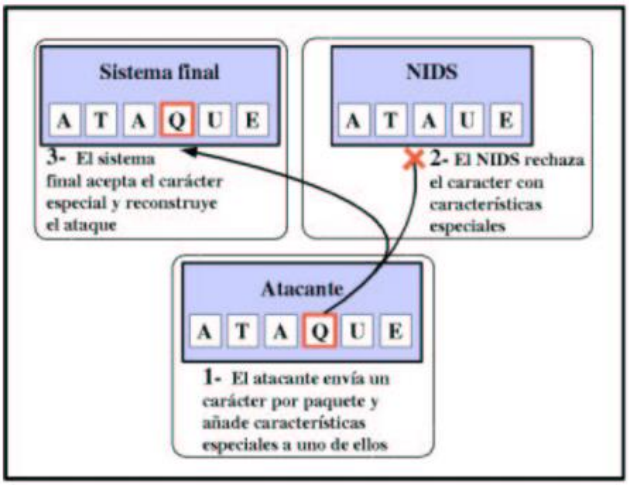


Fuente: Mira Alfaro José Emilio. Implantación de un sistema de detección de intrusos en la universidad de valencia. Valencia, España. Universidad de valencia. Facultad de informática. 26 p.

4.6.2 Evasión: Un sistema final puede aceptar un paquete que un IDS rechace. La figura 5 ilustra un ejemplo de este ataque.

El ataque de evasión provoca que el IDS vea un flujo diferente que el sistema final. Esta vez, sin embargo, el sistema final toma más paquetes que el IDS, y la información que el IDS pierde es crítica para la detección del ataque[8].

Figura 5. Ataque de evasión.



[8] Mira Alfaro José Emilio. Implantación de un sistema de detección de intrusos en la universidad de valencia. Valencia, España. Universidad de valencia. Facultad de informática. 25-27 p.

Fuente: Mira Alfaro José Emilio. Implantación de un sistema de detección de intrusos en la universidad de valencia. Valencia, España. Universidad de valencia. Facultad de informática. 27p.

5. DISEÑO METODOLÓGICO

La investigación se basará en la metodología de planeación, conducción, diseño y creación de investigación, planteada por Vaishnavi & kuechler la cual se compone de cinco pasos:

- **Conocimiento del problema:** Es el reconocimiento y articulación de un problema, el cual puede venir de estudiar la literatura donde los autores identifican las áreas para futuras investigaciones acerca de nuevos hallazgos en otras disciplinas, o de clientes que expresan la necesidad de algo o de investigaciones en otros campos o de nuevos desarrollos en tecnología.

- **Posibles soluciones:** Implica un salto creativo de la curiosidad sobre el problema de ofrecer una idea muy preliminar de cómo el problema podría resolverse.

- **Desarrollo:** Es donde la idea tentativa es diseñada o implementada, que está este bien depende en el tipo de dispositivo tecnológico que se ha propuesto, por ejemplo, un algoritmo podría necesitar la construcción de una prueba formal. Una nueva interfaz de usuario que incorpora nuevas teorías acerca de la cognición humana, la cual requiere un desarrollo de software. Un método de desarrollo de sistema necesita ser capturado en un manual que pueda entonces ser seguido en un sistema de desarrollo de proyectos.

- **Evaluación:** Examina el desarrollo de la solución dada y busca una evaluación de su valor y desviaciones sobre las expectativas.

- **Conclusiones:** Es donde el resultado del proceso de diseño es consolidado y redactado. El conocimiento ganado es identificado, junto con todos los cabos sueltos - inesperados resultados anómalos aún no se puede explicar y podría ser objeto de nuevas investigaciones[9].

[9] Oates, Briony. Researching Information Systems and computing. Thousand Oaks, california 91320, SGE publications inc, 2006. 111 p.

6. CONOCIMIENTO DEL PROBLEMA

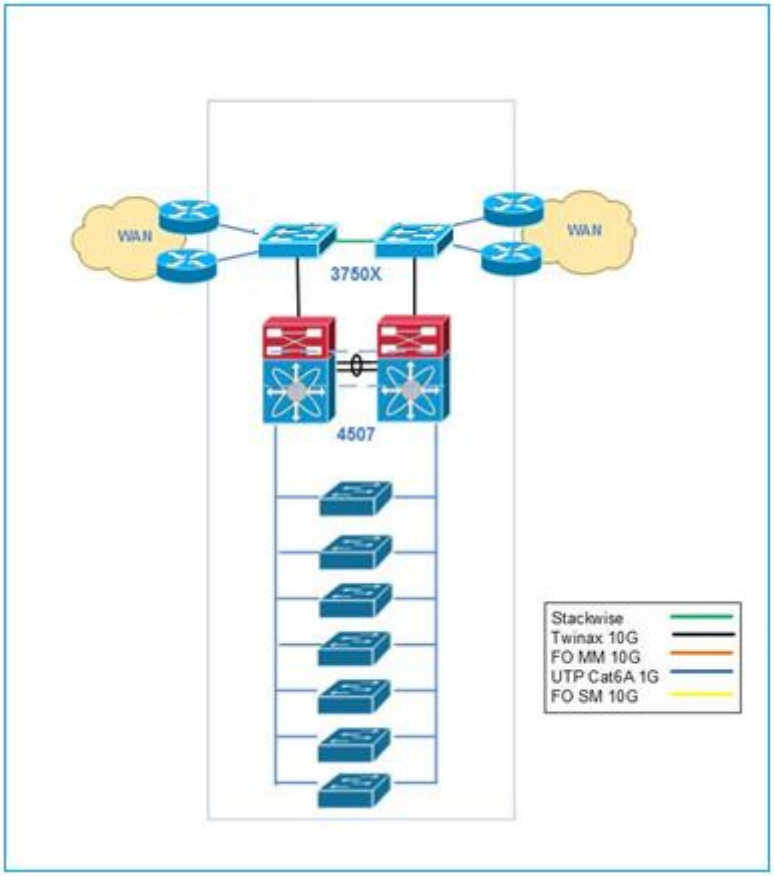
6.1 ESTADO ACTUAL DE LA RED

6.1.1 Capa de acceso: En esta capa se conectan los dispositivos finales como PCs, IP Phones, Printers. Actualmente se cuentan con switches CISCO Catalyst 2960 para realizar la gestión de acceso a la red de estos dispositivos finales.

6.1.2 Capa de distribución: En la capa de distribución se realiza filtrado de flujo de tráfico, políticas control de acceso, enrutamiento entre vlan. Para el funcionamiento de esta capa se cuenta con un switch CISCO 4507 R+E que permite desempeñar todas las funciones mencionadas anteriormente.

6.1.3 Capa de núcleo: En esta capa se maneja el enrutamiento, se encuentran dos switches 3750 de borde que están interconectados con los routers del proveedor, como se puede observar en la figura 6.

Figura 6. Diagrama general de red



Fuente: Autor

6.2 DESCRIPCIÓN FUNCIONAL

6.2.1 Seguridad en la red: En la capa de enlace los switches CISCO 2960 tienen configurado las funcionalidades de port security, arp inspection con el fin de evitar accesos no autorizados y ataques informáticos como mac flooding, arp spoofing o man in the middle.

En la capa de red, el switch 4507 R+E es el encargado de segregar las redes por medio de VLANS, manejar el enrutamiento intervlan y realizar un filtro básico de tráfico por medio de listas de acceso ACL.

En la capa de transporte se manejan dos UTM Fortinet trabajando en alta disponibilidad, cumple con funciones de firewall, antivirus, control de contenido y aplicaciones

En las terminales se cuenta con la solución de antivirus McAfee.

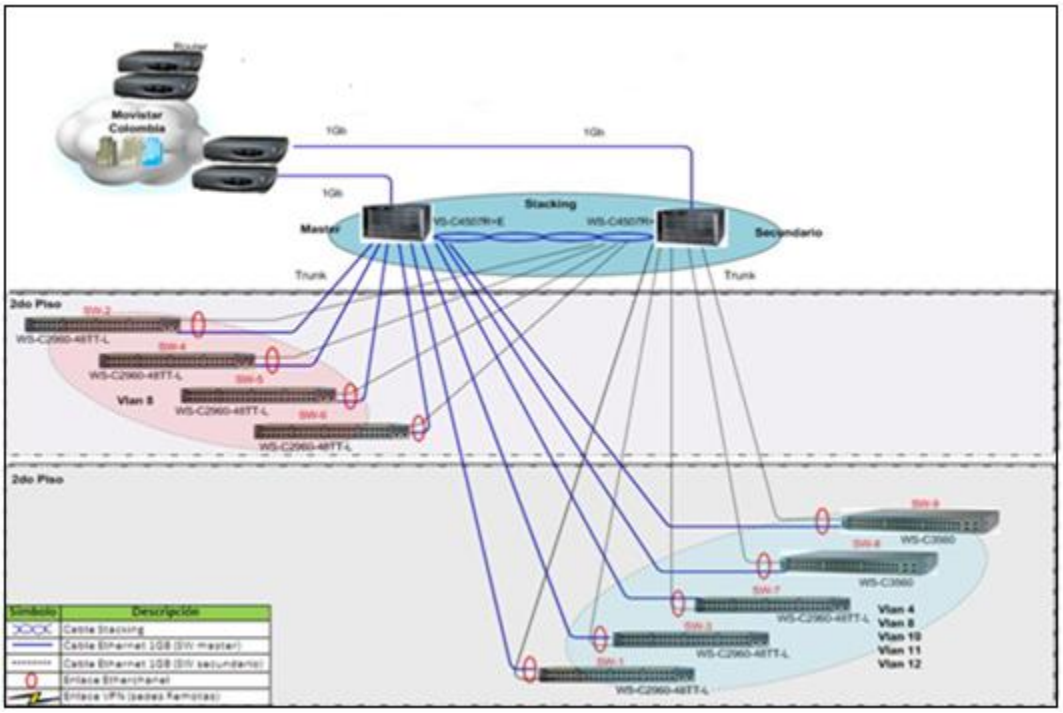
6.2.2 Switching: Se ha configurado el switch Core como el Root para todas las VLANs utilizando el Rapid Per Vlan Spanning-Tree Plus de CISCO (RPVST+), los switches CISCO de acceso también deben tener configurado RPVST+. STP estándar presenta tiempos de reconvergencia de hasta 30 segundos, RPVST+ disminuye los tiempos de reconvergencia al mínimo ante cambios en la topología.

Spanning-Tree Protocol (STP) es un protocolo de capa 2 del modelo OSI que asegura a través del uso de algoritmos una topología LAN libre de bucles. Spanning- Tree requiere que dentro de la topología se designe a un switch como raíz o root, que debe ser el switch core en una topología jerárquica. Tomando como referencia a este equipo es que se realizan los cálculos de rutas de menor coste desde todos los demás switches, bloqueando los puertos de rutas alternas que puedan generar bucles infinitos en la red.

6.2.3 Switch 4507 R+E: Este switch tiene una capacidad de conmutación de alto rendimiento y por la posición clave que ocupa en la red posee redundancia a nivel de hardware, cada uno de los switches de acceso se conecta a este, en algunos casos con dos enlaces de capacidad gigabit por segundo (1Gbps) formando un solo enlace lógico de una capacidad de dos gigabits por segundo (2Gbps) utilizando la funcionalidad de Agregación de Enlace (Link Aggregation). Los enlaces utilizados para este fin son de cobre UTP.

El diseño funcional de esta topología es ilustrado en la figura 7.

Figura 7. Diagrama de red



Fuente: Autor

6.3 EQUIPOS DE RED ACTIVOS

Cuadro 1. Inventario equipos de red

Nombre equipo	Marca	IP	Ubicación
SWCP1A1	WS-C2960-48TT-L	10.X.X.X	Piso 1 Rack A
SWCP1A2	WS-C2960-48TT-L	10.X.X.X	Piso 1 Rack A
SWCP1A3	WS-C2960-48TT-L	10.X.X.X	Piso 1 Rack A
SWCP1A4	WS-C2960-48TT-L	10.X.X.X	Piso 1 Rack A
SWCP1A5	WS-C2960-48TT-L	10.X.X.X	Piso 1 Rack A
SWCP1A6	WS-C2960-48TT-L	10.X.X.X	Piso 1 Rack A
SWCP1A7	WS-C2960-48TT-L	10.X.X.X	Piso 1 Rack A
SwitchCoreBlade	WS-C4507R+E	10.X.X.X	Data Center Rack D
SWCFW	WS-C3750G-24T-S	10.X.X.X	Data Center Rack D
	WS-C3750G-24T-S		Data Center Rack D
Fuente: Autor			

6.4 SERVIDORES ACTIVOS

A continuación, se mencionan todos los servidores y su rol en la red.

Cuadro 2. Servidores y servicios

MARCA	ROL	IP	Sistema Operativo y servicios
DELL	Aplicación web BBDD	10.X.X.X	Windows server 2003 SQL server 2008 IIS 7.0
DELL	*Intranet *Carpetas compartidas	10.X.X.X	Windows server 2003 IIS 7.0
HP	WSUS	10.X.X.X	Windows server 2003
HP	Active directory	10.X.X.X	Windows server 2003
HP	DHCP	10.X.X.X	Windows server 2003
Fuente: Autor			

6.5 DIRECCIONAMIENTO IP

A continuación, se ilustra el direccionamiento usado en la red.

Cuadro 3. Direccionamiento jerárquico de red

Nombre VLAN	#VLAN	Direccionamiento	Gateway
Gestión	VLAN1	10.X.X.X/24	10.X.X.X
Servidores	VLAN2	10.X.X.X/24	10.X.X.X
Recursos Humanos	VLAN3	10.X.X.X/25	10.X.X.X
Contabilidad	VLAN4	10.X.X.X/25	10.X.X.X
Gerencia	VLAN5	10.X.X.X/25	10.X.X.X
Tecnología	VLAN6	10.X.X.X/24	10.X.X.X
Wifi	VLAN7	10.X.X.X/25	10.X.X.X
Fuente: Autor			

6.6 ANÁLISIS DE RIESGOS

6.6.1 Identificación de activos: En el proceso de identificación, se seleccionaron tres activos que son críticos para la operación, según lo manifestó el área de IT.

- **Aplicativo web:** Este aplicativo es usado para el manejo de clientes (crm).
- **Directorio Activo:** En este servidor se encuentra el controlador de dominio.
- **Switch de core:** Dispositivo capa tres donde se encuentran interconectados todos los equipos que se encuentran en la capa de distribución.

6.6.2 Identificación de Amenazas: A continuación, se relacionan las amenazas presentadas.

Cuadro 4. Identificación de amenazas

Activos	Amenazas
Aplicativo WEB	Ataque informático
Servidor directorio activo	Ataque informático
Switch de Core	Ataque informático
Fuente: Autor	

6.6.3 Identificación de riesgos: A continuación, se relacionan los riesgos presentados.

Cuadro 5. Identificación de riesgos

Activos	Riesgos
Aplicativo WEB	R1: Divulgación de Información.
Servidor directorio activo	R2: Indisponibilidad en los servicios
Switch de Core	R3: Indisponibilidad en los servicios
Fuente: Autor	

6.7 ANÁLISIS Y EVALUACIÓN DE RIESGOS

Para el análisis y evaluación de los riesgos se deben tener en cuenta dos variables IMPACTO Y PROBABILIDAD, ya que normalmente el riesgo es igual a la probabilidad por el impacto. Estas dos variables pueden ser calculadas o medidas cuantitativamente si se hace referencia a valores numéricos como dinero, semi-cuantitativo si se hace referencia a un valor numérico combinando con escalas asignadas al riesgo, cualitativo si solo se asignan valores a las escalas como baja, media y alta.

En el caso de SilverIT se usará un esquema cualitativo en donde el impacto manejará las siguientes escalas:

- Catastrófica (5).
- Mayor (4).
- Moderada (3).
- Menor (2).
- Insignificante (1).

La probabilidad maneja las siguientes escalas:

- Casi certeza (5).
- Probable (4).
- Posible (3).
- Improbable (2).
- Raro (1).

Teniendo en cuenta las vulnerabilidades, amenazas y riesgos identificados anteriormente, se procede a realizar la correspondiente matriz que permite evaluar el riesgo para cada activo, como se ilustra en la figura 8.

Figura 8. Matriz de riesgo

Nivel Impacto					
Catastrófica					
Mayor				R1-R2-R3	
Moderada					
Menor					
Insignificante					
	Raro	Improbable	Posible	Probable	casi certeza
	Probabilidad				
Los niveles de riesgo definidos son: Alto, medio y bajo.					

Fuente: Autor

La matriz anterior refleja que los riegos R1, R2, R3, presentan un nivel de riesgo alto.

6.8 TRATAMIENTO DEL RIESGO

Existen varias formas de tratar el riesgo[10] las cuales son:

- **Reducirlo:** Se basa en la aplicación de algún control que permita minimizar el riesgo.
- **Aceptarlo:** Permitir que el riesgo se materialice.
- **Rechazarlo:** No proceder con el proyecto o la actividad que incorporaría el riesgo, o escoger medios alternativos para la actividad, que logren el mismo resultado y no incorporen el riesgo detectado.
- **Transferirlo compartirlo:** se trata de subcontratar a una persona o empresa para que ellos realicen la actividad que representa el riesgo.

Con este diseño se pretende reducir el riesgo a un nivel medio.

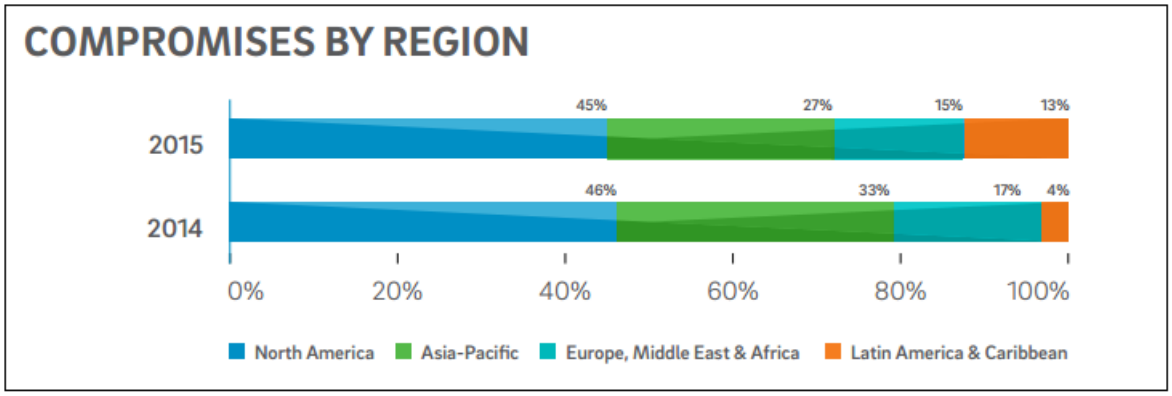
[10] Departamento administrativo de la función pública (2004). Guía de administración del riesgo [online] Disponible en internet agosto 22 de 2016 http://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CDQQFjAD&url=http%3A%2F%2Fwww.ufps.edu.co%2Fufpsnuevo%2Fproyectos%2Fmeci%2Fdocumentos%2Fplanes%2FGUIA_ADMINISTRACION_DEL_RIESGO_-_DAFP.pdf&ei=mv9wVbSLJKqQsQT2wIC4Dg&usg=AFQjCNGbef-HIpqz1tcsXuNVVzzD3pltgg&bvm=bv.95039771,d.b2w&cad=rja

6.9 ATAQUES INFORMÁTICOS

Según la compañía estadounidense TRUSTWAVE reconocida por su lucha contra la ciberdelincuencia, en su reporte anual "**trustwave global security report 2016**" devela varias estadísticas de gran interés como:

- Estadísticas de incidentes presentados por región, comparativos años 2015, 2014. Estas estadísticas son derivadas de varios de cientos de investigaciones llevadas a cabo por el equipo de spyder labs. Se observa un gran crecimiento de incidentes en América Latina según la figura 9.

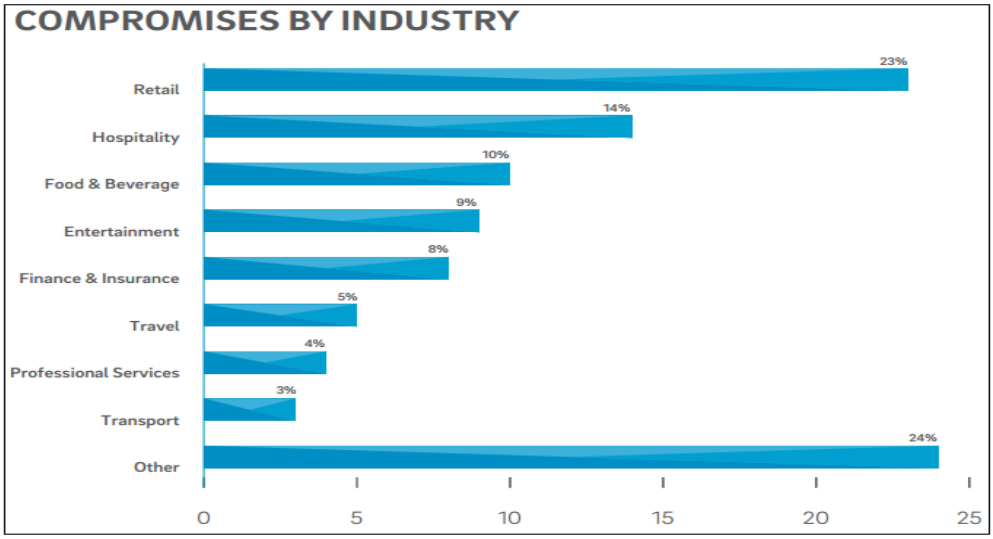
Figura 9. Porcentaje incidentes seguridad informática por región



Fuente: Andrews, Brett et al. 2016 Trustwave Global Security report, Trustwave holdings, chicago 2016. 13 p.

- La siguiente estadística muestra el porcentaje de incidentes presentados a diversos sectores de la industria, donde todos han sido blancos de ciberataques como se puede ver en la figura 10. También se puede resaltar que para los delincuentes informáticos no existe compañía pequeña y mucho menos una industria que no les parezca interesante atacar.

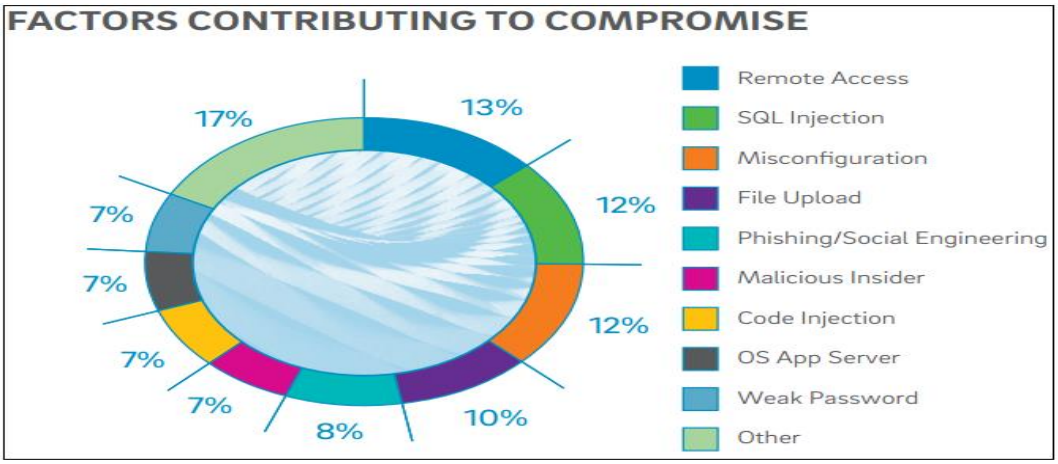
Figura 10. Porcentaje incidentes seguridad informática por industria.



Fuente: Andrews, Brett et al. 2016 Trustwave Global Security report, Trustwave holdings, chicago 2016. 13 p.

- Por último, una de las estadísticas más importantes, la figura 11 muestra el porcentaje por cada vector de ataque lo cual deja entrever que firmas se pueden ser configuradas en el IDS.

Figura 11. Porcentaje según el tipo de ataque informático usado



Fuente: Andrews, Brett et al. 2016 Trustwave Global Security report, Trustwave holdings, chicago 2016. 23 p.

Teniendo en cuenta la información anterior, el diseño se enfoca en los ataques remotos y de SQL injection ya que son los más populares a la hora de atacar sistemas de información.

6.9.1 SQL injection: Structures Query Language (SQL) es básicamente un lenguaje textual que habilita la interacción con un servidor de bases de datos. Los comandos SQL como INSERT, RETRIEVE, UPDATE y DELETE son usados para realizar operaciones en una base de datos. Programadores usan estos comandos para manipular los datos en el servidor de base de datos.

SQL injection es definido como una técnica que toma ventajas de entradas que no manejan validaciones e inyección de comandos SQL a través de una aplicación web que es ejecutada en un back-end base de datos. Programadores usan comandos SQL secuenciales con parámetros client-supplied haciendo esto más fácil para que los atacantes inyecten código. Atacantes pueden fácilmente ejecutar aleatoriamente querys SQL sobre las bases de datos a través de la aplicación. Los atacantes usan esta técnica ya sea para ganar acceso no autorizado a la base de datos o recuperar información directamente de esta.

6.9.1.1 Objetivos SQL injection: Basados en la aplicación y como estos procesos user-supplied data, SQL injection puede ser usado para llevar a cabo:

- **Evasión de autenticación:** Aquí el atacante puede entrar en la red sin proveer algún dato de autenticación como usuario o clave y puede ganar acceso sobre la red.
- **Revelación de información:** Después del ingreso no autorizado a la red, el atacante puede tener acceso a información sensible almacenada en la base de datos.
- **Compromiso de integridad de la información**: El atacante cambia el contenido del sitio web e introduce contenido malicioso en este.
- **Ejecución código remoto:** Un atacante puede modificar, eliminar o crear datos o incluso puede crear nuevas cuentas con permisos de administrador para que pueda acceder a todas las carpetas compartidas. Este también puede comprometer el sistema operativo del servidor.[11]

[11] Ec council CEHv8 Module 14 SQL Injection [Diapositivas], 2014.

6.9.1.2 Ejemplo de SQL injection: A continuación, se observa cómo se genera una inyección de código, insertando un carácter que no fue validado por el desarrollador, lo que permite que se ejecute en el motor de bases de datos una consulta inadecuada.

Figura 12. Ejemplo SQL injection

En SQL:

```
select id, firstname, lastname from authors
```

Si uno proporciona:

```
Firstname: evil'ex
Lastname: Newman
```

La cadena de consulta se convierte en:

```
select id, firstname, lastname from authors where forename = 'evil'ex' and surname ='newman'
La cual la base de datos intenta ejecutar como:
```

```
Incorrect syntax near il' as the database tried to execute evil.
```

Una versión segura de la anterior instrucción SQL podría ser codificada en Java como:

```
String firstname = req.getParameter("firstname");
String lastname = req.getParameter("lastname");
// FIXME: do your own validation to detect attacks
String query = "SELECT id, firstname, lastname FROM authors WHERE forename = ? and surname = ?";
PreparedStatement pstmt = connection.prepareStatement( query );
pstmt.setString( 1, firstname );
pstmt.setString( 2, lastname );
try
{
        ResultSet results = pstmt.execute( );
}
```

Fuente: owasp, [online] Disponible en internet, septiembre 2016 <url: https://www.owasp.org/index.php/SQL_Injection>.

6.9.2 Ataques de acceso remoto: Un ataque remoto, es aquel que usa cualquier protocolo de internet para interactuar con su objetivo, por lo general siempre se hace con el fin de explotar alguna vulnerabilidad existente identificada con el fin de ingresar al sistema y tener control de este o simplemente robar información.

Estos ataques generalmente son desplegados a equipos desprotegidos en internet o que tiene software o sistemas operativos desactualizados ya que de esta forma es más fácil para el pirata informático generar sus vectores de ataque y tener éxito, estos ataques se llevan a cabo mediante herramientas y software diseñado para estos fines.

En los ataques remotos, inicialmente, el atacante no tiene control sobre su objetivo. Es por esta razón, que usan técnicas de ingeniería social para que las personas los ayuden inconscientemente a darle el control como por ejemplo con el envío de un correo que promocione una oferta y contenga malware.

6.9.2.1 Objetivos de un ataque remoto: Algunos de los principales objetivos de un ataque remoto son los siguientes:

- Lograr acceso a un sistema informático específico.
- Robar información de cualquier tipo.
- Hacerse con números de tarjetas de crédito.
- Obtener acceso a cuentas bancarias.
- Utilizar el sistema infectado como “rebote” en otros ataques informáticos.
- Usar los recursos de la máquina infectada.

6.9.2.2 Categorías ataques de acceso remoto: Existen muchas técnicas que permiten a los atacantes comprometer sistemas remotos. Se dividen en varias categorías:

6.9.2.3 Ataques DoS: El principal objetivo de este ataque es evitar que los equipos o servicios no estén disponibles para sus usuarios ya sean internos o externos, un método común es que muchos equipos realicen peticiones de conexión a un mismo equipo y este no pueda soportar dicho volumen de peticiones lo cual lo hará colapsar, si este lo soporta, trabajara muy lentamente.

6.9.2.4 Envenenamiento DNS: Utilizando el envenenamiento DNS (Domain Name Server) los hackers pueden engañar a los usuarios para que estos sean redireccionados a páginas web falsas y así robar sus datos o para que descarguen virus o troyanos.

6.9.2.5 Exploración de puertos: La exploración de puertos se usa con el fin de identificar que puertos o servicios puede estar prestando un equipo, esta actividad puede revelar información relevante para la explotación de una vulnerabilidad, por eso los administradores prefieren dejar abiertos únicamente los puertos que son

necesarios para el funcionamiento del negocio, adicionalmente esta es una actividad legitima.

6.9.2.6 Desincronización de TCP: La desincronización TCP tiene como objetivo desincronizar la victima con el servidor para que el atacante se conecte con la secuencia numérica acertada y realizar un secuestro de sesión.

6.9.2.7 Ataques ICMP: ICMP (Internet Control Message Protocol) es un protocolo muy importante y conocido ya que se usa con el fin de saber que equipos se encuentran con vida dentro de una red, se puede usar para desencadenar ataques DoS o exploración de puertos[12].

7. POSIBLES SOLUCIONES

[12] **ESET [online] Disponible en internet, agosto 2016. <URL:http://soporte.eset-la.com/kb2907/?locale=es_ES>.**

Existen diversas soluciones en el mercado que pueden ayudar a minimizar el nivel de probabilidad que una amenaza sea materializada, la compañía se basa en las siguientes variables para la selección de la solución:

- El producto seleccionado debe tener la capacidad de detectar ataques SQL injection y ataques remotos, en los cuales también se contemplan las plataformas usadas actualmente.
- El producto seleccionado debe tener la capacidad de detectar ataques en tiempo real.
- El producto se debe adaptar fácilmente a la infraestructura actual.
- El valor de la inversión debe ser baja para implementación y mantenimiento de la misma.

7.1 SNIFFER

Un sniffer es un analizador de protocolos el cual captura todas las tramas, paquetes y segmentos de red para que puedan ser analizados, el sniffer se puede usar para monitorear todo el tráfico de red de la organización, pero este mecanismo es obsoleto ya que el solo ve el trafico mas no genera alarmas por sí solo, es indispensable contar con varias personas las cuales deben estar revisando el trafico lo cual lo hace de este un trabajo dispendioso generando costos adicionales.

7.2 PREVENCIÓN DE INTRUSOS

Permite detectar y contener ataques en línea, actualmente en el mercado existen soluciones de prevención de intrusos de diferentes fabricantes como Fortinet, Checkpoint, CISCO, Palo Alto entre otras. Estas soluciones implicarían un alto nivel de inversión por lo cual no son una opción viable en este momento para la compañía.

7.3 DETECTOR DE INTRUSOS

Permite detectar los ataques en línea generando alarmas para que los administradores puedan tomar acciones reactivas. A continuación se realiza una comparación entre un IPS e IDS, lo cual ayudara a entender la funcionalidad de cada uno con sus ventajas y desventajas como lo muestra el cuadro 6.

Cuadro 6. Comparación IDS/IPS

IPS	IDS
Detecta y protege	Detecta.
El trafico fluye a través de él.	Requiere un puerto espejo.
Puede impactar el desempeño de la red.	No impacta el desempeño de la red.
Puede impactar la disponibilidad de la red.	No impacta disponibilidad de la red.
Fuente: Autor	

7.4 SELECCIÓN SOLUCIÓN

Basado en la información recopilada y analizada se decidió implementar SNORT, SNORT es un sistema de detección y prevención de intrusos de código abierto capaz de analizar tráfico en tiempo real y realizar el registro de paquetes[13].

Se eligió esta solución por sus bajos costos de implementación y por ser un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida.

Este IDS implementa un lenguaje de creación de reglas flexible, potente y sencillo. Durante su instalación ya este provee de cientos de filtros o reglas para backdoor, DDoS, finger, FTP, ataques web, CGI, nmap entre otros.

Snort utiliza la biblioteca estándar libcap y tcpdump como registro de paquetes en el fondo, trabaja bajo licencia GPL y es gratuito para sistemas operativos Linux y Windows, tiene una gran cantidad de filtros y unas de las cosas que más atrae a los usuarios es la cantidad de firmas existentes, adicional se cuenta con una comunidad entera que mantiene las reglas actualizadas y comparte sus conocimientos lo cual convierte a Snort en una herramienta muy popular, actualizada y robusta[14].

7.5 DISMINUCIÓN DEL RIESGO

[13] SNORT, [online] Disponible en internet, agosto 2016. <URL:www.snort.org

[14] Wikipedia, [online] Disponible en internet, agosto 2016 https://es.wikipedia.org/wiki/Snort

Con este diseño el riesgo disminuirá a un nivel medio como se ilustra en la figura 13, ya que con la configuración del sistema de detección de intrusos la probabilidad de que los ataques informáticos tengan éxito será menor.

Figura 13. Matriz riesgo Residual

Nueva Matriz Análisis de Riesgo con el IDS para los riesgos R1, R2 y R3					
Nivel Impacto					
catastrófica (5)					
mayor (4)			R1-R2-R3		
moderada (3)					
menor (2)					
insignificante (1)					
	Raro (1)	Improbable (2)	Posible (3)	Probable (4)	casi certeza (5)
	Probabilidad				
Los niveles de riesgo definidos son: Alto, medio y bajo.					

Fuente: Autor

8. DESARROLLO

8.1 FACTORES DE DISEÑO

Para el diseño se tuvieron en cuenta los siguientes factores:

- Identificación de los activos y generación de sus análisis de riesgo respectivo.
- Reporte generado por Trustwave el cual muestra cuáles son los ataques informáticos más usuales.
- Versiones de sistemas operativos, motores de bases de datos, servicios prestados.
- Infraestructura utilizada, direccionamiento de red, VLANS.
- La solución seleccionada, en este caso Snort.
- Necesidad de detectar ataques informáticos en la red de área local.

8.2 CONFIGURACIÓN INTERFACES DE RED

El IDS cuenta con dos tarjetas de red, la primera tarjeta de red funcionará en modo promiscuo con el fin que pueda escuchar todo el tráfico de red, la segunda tarjeta de red permitirá realizar la administración del IDS, si solo se usa una tarjeta de red en modo promiscuo la administración del IDS será dispendiosa ya que no se podrá acceder al mismo desde un lugar remoto, obligatoriamente se debe estar en el mismo lugar donde se encuentra el IDS.

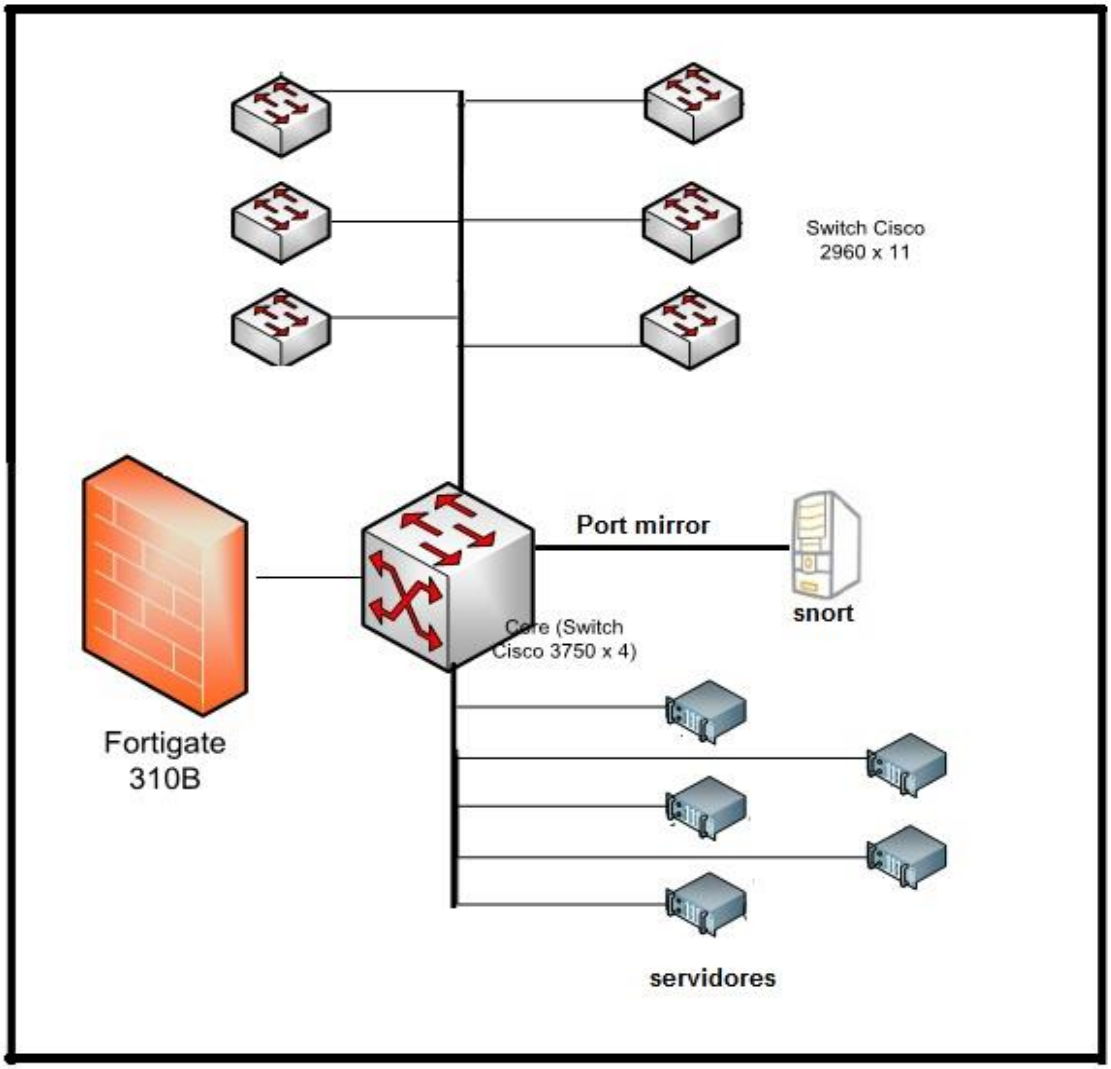
8.3 UBICACIÓN SISTEMA DETECCIÓN DE INTRUSOS

Como se tiene la necesidad de generar un monitoreo sobre la red de área local, la mejor ubicación para poner el IDS es en el switch core CISCO 4705 R+E, ya que por este dispositivo pasa todo el tráfico de la red de área local, por ende, cualquier petición que se realice o cualquier ataque que se genere hacia estos tendrá que pasar por dicho dispositivo. Para que el IDS pueda escuchar el tráfico, en el switch core se configura un puerto espejo, un puerto espejo o port mirroring es utilizado con un switch de red para enviar copias de paquetes de red vistos en un puerto del switch (o una VLAN entera) a una conexión de red monitoreada en otro puerto del switch.

Esto es comúnmente utilizado para aplicaciones de red que requieren monitorear

el tráfico de la red, tal como un IDS (Intrusion Detection System)[15]. Bajo este concepto el puerto GI0/40 del switch core trabajará como puerto espejo, todo el tráfico que vaya hacia la vlan de servidores será replicado en el puerto GI0/40 en el cual estará conectado el IDS SNORT como se observa en la figura 14. Únicamente se hará espejo del trafico dirigido hacia la vlan de servidores con el fin de evitar falsos positivos y saturación del IDS.

Figura 14. Ubicación snort en la red de SilverIT



Fuente: Autor

[15] Wikipedia, [online] Disponible en internet, septiembre 2016 url:https://es.wikipedia.org/wiki/Puerto_espejo.

8.4 ARQUITECTURA SNORT

La arquitectura de Snort está compuesta de los siguientes módulos:

- **Módulo de captura del tráfico:** Es el encargado de capturar todos los paquetes de la red utilizando la librería libpcap.

- **Decodificador:** Se encarga de formar las estructuras de datos con los paquetes capturados e identificar los protocolos de enlace, de red, etc.

- **Preprocesadores:** Permiten extender las funcionalidades preparando los datos para la detección. Existen diferentes tipos de preprocesadores dependiendo del tráfico que se quiere analizar (por ejemplo, existen los preprocesadores http, telnet).

- **Motor de Detección:** Analiza los paquetes en base a las reglas definidas para detectar los ataques.

- **Archivo de Reglas:** Definen el conjunto de reglas que regirán el análisis de los paquetes.

- **Plugins de detección:** Partes del software que son compilados con Snort y se usan para modificar el motor de detección.

- **Plugins de salida:** Permiten definir qué, cómo y dónde se guardan las alertas y los correspondientes paquetes de red que las generaron. Pueden ser archivos de texto, bases de datos, servidor syslog, etc.

Los módulos mencionados anteriormente se ven representados en la figura 15.

Figura 15. Estructura snort

Fuente: Galindo Jimenez Carlos. Diseño y Optimizacion de un sistema de detección de intrusos hibrido. Almeria, España. Universidad de Almeria. Facultad de informática. 14 p.

8.5 REGLAS SNORT

Las reglas de snort son divididas en dos secciones lógicas, el encabezado de la regla y las opciones.

8.5.1 Encabezado de la regla: El encabezado contiene la acción, protocolo, ip origen, ip destino, puerto origen y puertos destino. Las opciones contienen mensajes de alerta e información sobre la cual partes de un paquete pueden ser inspeccionadas para determinar si una acción puede ser tomada.

8.5.1.1 Protocolos: El siguiente campo en una regla es el protocolo, debe ser uno de los cuatro que Snort puede analizar actualmente: TCP, UDP, ICMP o IP.

8.5.1.2 Direcciones IP y puerto: El siguiente campo hace referencia a la dirección IP y el puerto de origen, tras el operador de dirección también se especifican la dirección IP y el puerto de destino.

8.5.1.3 Operador de dirección: Indica la orientación o dirección del tráfico sobre el que se aplicará la regla. Puede ser “->” o “<>” (bidireccional).

8.5.2 Acciones de la regla: El encabezado de la regla contiene la información que define el quien donde y porque de un paquete, así como el que hacer en el

evento en que unos paquetes con todos los atributos indiquen que la regla debe aparecer. El primer elemento en una regla es la acción.

Ejemplo: Alert tcp any any -> 192.168.1.0/24 111\ (content:"|00 01 86 a5|"; msg:"mount access";)

La acción dice que hacer cuando se encuentra un paquete que coincide con los criterios establecidos[16].

Cuadro 7. Encabezados de las reglas en snort

Acción de la regla	Acción que ejecuta
alert	Genera una alerta usando el método elegido y luego registra el paquete en un log.
log	Registra el paquete en un log.
pass	Ignorar el paquete.
activate	Genera una alerta y luego activa otra regla dinámica.
dynamic	Permanece desactivada hasta que se activa con una regla "activate", luego actúa como una regla "log".
drop	Bloquea y registra el paquete en un fichero log.
reject	Bloquea el paquete, lo registra y luego envía un TCP reset si el protocolo es TCP o un "ICMP port unreachable" si el protocolo es UDP
sdrop	Bloquea el paquete, pero no lo registra en un log.
Fuente: Snort users manual	

8.5.2.1 Opciones de regla

Las opciones de las reglas forman el corazón del motor de detección de intrusiones de Snort, que combina facilidad de uso con potencia y flexibilidad. Todas las opciones de la regla Snort se separan unos de otros mediante el punto y coma (;). Las opciones clave son separados de sus argumentos con dos puntos (:).

[16] Galindo Jimenez Carlos. Diseño y Optimizacion de un sistema de detección de intrusos hibrido. Almeria, España. Universidad de Almeria. Facultad de informática 40-42 p.

Existen cuatro categorías de opciones de regla representadas en el cuadro 8.

Cuadro 8. Opciones específicas de las reglas en Snort

Opción	Acción
general	Estas opciones proveen información acerca de la regla, pero no tiene algún efecto durante la detección.
payload	Estas opciones buscan dentro del payload del paquete y pueden ser relacionados entre sí.
non-payload	Estas opciones no revisan los datos del payload.
post-detection	Estas opciones son desencadenan acciones específicas después que la regla fue alarmada.
Fuente: Snort users manual	

Posterior a estas se describen las principales opciones de las reglas en el cuadro 9.

Cuadro 9. Opciones principales de las reglas en snort

Opción	Acción
Msg	Informa al motor de alerta que mensaje debe mostrar. Los caracteres especiales de las reglas como : y ; deben de colocarse dentro de la opción msg con el carácter.
Flow	Se usa junto con los flujos TCP, para indicar qué reglas deberían de aplicarse sólo a ciertos tipos de tráfico.
Content	Permite que Snort realice una búsqueda sensitiva para un contenido específico del payload del paquete.
Referent	Define un enlace a sistemas de identificación de ataques externos, como bugtraq, con id 788.
Classtype	Indica qué tipo de ataques intentó realizar el paquete. La opción classtype, usa las clasificaciones definidas en el archivo de configuración de Snort y que se encuentran en archivos como classification.config. La sintaxis del classification.config es: La prioridad es un valor entero, normalmente 1 es para prioridad alta, 2 media y 3 baja. La opción classification para el attempted-admin que aparece en classification.config, es la siguiente: config classification: attempted-admin,Attempted Administrator Privilege Gain,1

DIS	en combinación con la opción rev, únicamente identifica una regla Snort, correlacionando el ID de la regla individual con la revisión de la regla.
Fuente: Snort users manual	

8.6 MODOS DE INTERACCIÓN DE SNORT

Snort puede ser configurado para correr en tres modos:

- Sniffer, con lo cual simplemente lee los paquetes en la red y los muestra en pantalla.

- Packet Logger, guarda todos los registros de los paquetes en disco.

- Network Intrusion Detection System (NIDS), el cual realiza la detección y análisis sobre el tráfico de la red. Este es el modo más complejo de configurar[17].

En este caso el detector de intrusos funcionara como un NIDS.

8.7 CREACIÓN REGLAS IDS

Para la creación de reglas se tuvo en cuenta lo siguiente:

- El aplicativo web está basado sobre sistema operativo Windows server 2003, como motor de base de datos tiene SQL server 2008, teniendo en cuenta estas plataformas y el reporte de trustwave, deben ser implementadas reglas que permitan detectar ataques de SQL injection, no obstante, también se deben tener reglas para el sistema operativo y alguno de sus servicios como el IIS (internet information server).

- El servidor de directorio activo tiene sistema operativo windows server 2003, por ende, se deben establecer reglas que detecten ataques de acceso remoto para servidores Windows como denegación de servicio, envenenamiento de dns, ataques de smb, etc. Normalmente estos ataques se realizan por medio de exploits ya que son muy populares, como se pudo ver en la etapa de conocimiento.

[17] **SNORT setup guide, [online] Disponible en internet, agosto 2016.**
<URL:https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/090/original/Snort_2.9.8.x_on_Ubuntu_12-14-15.pdf?AWSAccessKeyId=AKIAIXACIED2SPMSC7GA&Expires=1471903229&Signature=CEgCbj0IDMj8JqwirzOOZXT9bic%3D>.

8.7.1 Reglas SQL injection: A continuación, se relacionarán las reglas que se pondrán para detección de ataques basados en SQL injection.

- alert tcp $SQL_SERVERS 1433 -> $EXTERNAL_NET any (msg:"SQL sa login failed"; flow:to_client,established; content:"Login failed for user 'sa'"; fast_pattern:only; metadata:policy balanced-ips drop, policy connectivity-ips drop, policy security-ips drop, ruleset community; reference:bugtraq,4797; reference:cve,2000-1209; reference:nessus,10673; classtype:unsuccessful-user; sid:688; rev:16;)

- alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"SQL generic SQL with comments injection attempt - GET parameter"; flow:to_server,established; content:"/*"; http_uri; content:"*/"; http_uri; pcre:"/(update|exec|insert|union)[^\/\\]*\/*.**\//Uis"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:url,www.securiteam.com/securityreviews/5DP0N1P76E.html; classtype:web-application-attack; sid:16431; rev:5;)

- alert tcp any any -> $SQL_SERVERS 1433 (msg:"SQL WinCC DB default password security bypass attempt"; flow:to_server,established; content:"WinCCConnect"; content:"2WSXcder"; distance:0; metadata:policy balanced-ips drop, policy security-ips drop; reference:cve,2010-2772; reference:url,support.automation.siemens.com/WW/view/en/43876783; classtype:attempted-user; sid:17044; rev:3;)

- alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SQL 1 = 0 - possible SQL injection attempt"; flow:to_server,established; content:"1=0"; fast_pattern:only; http_uri; pcre:"/(and|or)[\s\x2F\x2A]+1=0/Ui"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:url,ferruh.mavituna.com/SQL-injection-cheatsheet-oku/; classtype:web-application-attack; sid:19440; rev:8;)

- alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SQL 1 = 1 - possible SQL injection attempt"; flow:to_server,established; content:"1=1"; fast_pattern:only; http_uri; pcre:"/(and|or)[\s\x2f\x2A]+1=1/Ui"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:url,ferruh.mavituna.com/SQL-injection-cheatsheet-oku/; classtype:web-application-attack; sid:19439; rev:8;)

- alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SQL 1 = 1 - possible SQL injection attempt"; flow:to_server,established; content:"|27|1|27|=|27|1"; fast_pattern:only; http_client_body; metadata:policy balanced-ips drop, policy security-ips drop, service http;

reference:url,ferruh.mavituna.com/SQL-injection-cheatsheet-oku/; classtype:web-application-attack; sid:27288; rev:3;)

- alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SQL 1 = 1 - possible SQL injection attempt"; flow:to_server,established; content:"1=1";fast_pattern:only;http_client_body;pcre:"/or[\s\x2f\x2A]+1=1/Pi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:url,ferruh.mavituna.com/SQL-injection-cheatsheet-oku/; classtype:web-application-attack; sid:27287; rev:3;)

- alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SQL 1 = 1 - possible SQL injection attempt"; flow:to_server,established; content:"%271%27%3D%271"; fast_pattern:only; http_client_body; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:url,ferruh.mavituna.com/SQL-injection-cheatsheet-oku/; classtype:web-application-attack; sid:30041; rev:2;)

- alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SQL 1 = 1 - possible SQL injection attempt"; flow:to_server,established; content:"1%3D1"; fast_pattern:only; http_client_body; pcre:"/or\++1%3D1/Pi"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:url,ferruh.mavituna.com/SQL-injection-cheatsheet-oku/; classtype:web-application-attack; sid:30040; rev:2;)

- alert tcp $SQL_SERVERS [1315,2315] -> $EXTERNAL_NET any (msg:"SQL IBM SolidDB initial banner"; flow:to_client,established; content:"IBM solidDB"; fast_pattern:only; flowbits:set,soliddb; flowbits:noalert; metadata:policy max-detect-ips drop; classtype:misc-activity; sid:23393; rev:5;)

- alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SQL url ending in comment characters - possible SQL injection attempt"; flow:to_server,established; content:"--"; fast_pattern:only; http_uri; pcre:"/(SELECT|UPDATE|INSERT)\x20+[^\r\n\x26]+--$/Ui"; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service http; reference:cve,2012-2998; reference:url,ferruh.mavituna.com/SQL-injection-cheatsheet-oku/; classtype:web-application-attack; sid:19438; rev:13;)

- alert tcp $EXTERNAL_NET any -> $HOME_NET 50000 (msg:"SQL IBM DB2 Universal Database xmlquery buffer overflow attempt"; flow:to_server,established; content:"xmlquery"; fast_pattern:only; content:"select "; nocase; pcre:"/select\s+xmlquery\s*\x28\s*(\x27|\x22)[^\x27\x22]{512}/smi"; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service drda, service mySQL; reference:bugtraq,29601;

reference:cve,2008-3854; classtype:attempted-user; sid:14991; rev:7;)

8.7.2 Reglas ataques remotos S.O Windows: A continuación, se relacionarán las reglas que se pondrán para detección de ataques remotos en windows.

- alert tcp $EXTERNAL_NET any -> OS-WINDOWS Microsoft Windows Calendar object heap corruption attempt"; flow:to_server,established; file_data; content:"|08 1A 02 E9 9E 48 80 43 BD D9 09 28 B3 91 21 AB 00 08 B7 7A 5C 56 19 34 E0 89 03 06 12 0D 04 20 01 01 02 03|"; fast_pattern:only; metadata:policy balanced-ips drop, policy security-ips drop, service smtp; reference:cve,2015-1673; reference:url,technet.microsoft.com/en-us/security/bulletin/ms15-048; classtype:attempted-user; sid:34402; rev:1;)

- alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"OS-WINDOWS Microsoft Windows Calendar object heap corruption attempt"; flow:to_client,established; file_data; content:"|08 1A 02 E9 9E 48 80 43 BD D9 09 28 B3 91 21 AB 00 08 B7 7A 5C 56 19 34 E0 89 03 06 12 0D 04 20 01 01 02 03|"; fast_pattern:only; metadata:policy balanced-ips drop, policy security-ips drop, service ftp-data, service http, service imap, service pop3; reference:cve,2015-1673; reference:url,technet.microsoft.com/en-us/security/bulletin/ms15-048; classtype:attempted-user; sid:34401; rev:1;)

- alert tcp $HOME_NET any -> any [137,139] (msg:"OS-WINDOWS Microsoft Windows SMB Microsoft Windows Remote Administration Protocol usage attempt"; flow:to_server,established; content:"LANMAN"; flowbits:set,file.lanman; flowbits:noalert; metadata:policy max-detect-ips drop, service netbios-ssn; classtype:misc-activity; sid:29514; rev:5;)

- alert tcp $HOME_NET any -> any [137,139] (msg:"OS-WINDOWS Microsoft Windows SMB Microsoft Windows Remote Administration Protocol usage attempt"; flow:to_server,established; content:"|5C 00|P|00|I|00|P|00|E|00 5C 00|L|00|A|00|N|00|M|00|A|00|N"; flowbits:set,file.lanman; flowbits:noalert; metadata:policy max-detect-ips drop, service netbios-ssn; classtype:misc-activity; sid:28425; rev:5;)

- alert tcp $HOME_NET any -> any [138,139,445] (msg:"OS-WINDOWS Microsoft Windows SMB RAP API NetServerEnum2 long server name buffer overflow attempt"; flow:to_server,established; content:"|68 00|WrLehD"; pcre:"/^[oz]/Ri"; content:"|01 00|"; within:2; distance:9; flowbits:set,netsenum; flowbits:noalert; metadata:policy max-detect-ips drop, service netbios-ssn; reference:bugtraq,54940; reference:cve,2012-1853; reference:url,osvdb.org/show/osvdb/84601;

reference:url,technet.microsoft.com/en-us/security/bulletin/MS12-054; classtype:attempted-dos; sid:23839; rev:15;)

- alert tcp $EXTERNAL_NET any -> $HOME_NET 3389 (msg:"OS-WINDOWS Microsoft Windows RemoteDesktop new session flood attempt"; flow:to_server,established; content:"|02 F0 80 7F 65|"; content:"|03 00|"; within:2; distance:-9; detection_filter:track by_src,count 10,seconds 3; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop; reference:cve,2012-0002; reference:url,technet.microsoft.com/en-us/security/bulletin/ms12-020; classtype:attempted-admin; sid:21570; rev:8;)

- alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"OS-WINDOWS Microsoft SilverLight ImageSource redefine flowbit"; flow:to_client,established; file_data; content:"|2E|findName|28 22|"; content:"|2E|ImageSource"; distance:0; pcre:"/var\s*(?P<imagebrush>\w+?)\x3b.*?(?P=imagebrush)\s*\x3d\s*[^\x3b\x2e]+\x2efindName\x28.*?(?P=imagebrush)\x2eImageSource\s*\x3d\s*[\x22\x21][^\x2e\x22\x21]+?[\x22\x21]/smi"; flowbits:set,imagesource.redefine; metadata:policy max-detect-ips drop, service ftp-data, service http, service imap, service pop3; classtype:misc-activity; sid:17113; rev:16;)

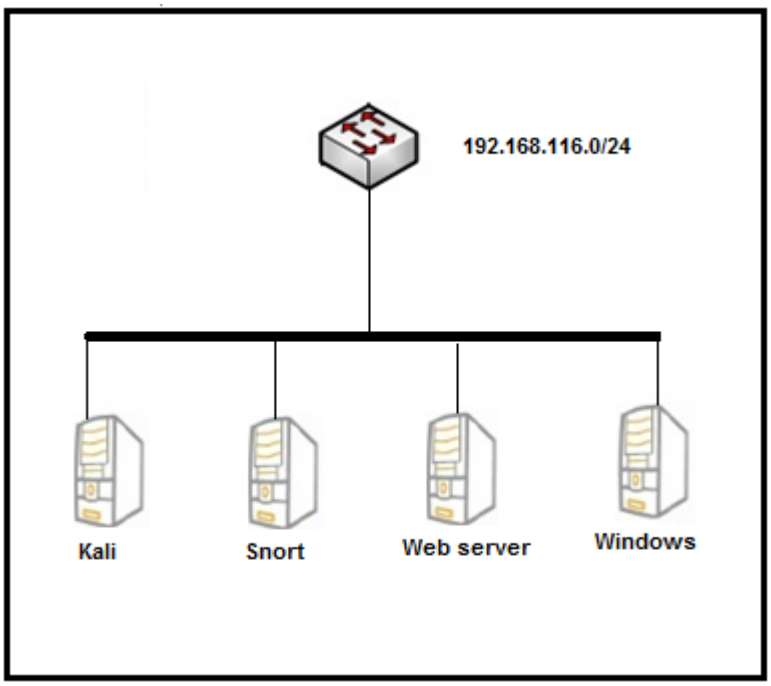
- alert tcp $EXTERNAL_NET any -> $HOME_NET [135,139,445,593,1024:] (msg:"OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrPathCanonicalize overflow attempt"; flow:to_server,established; dce_iface:4b324fc8-1670-01d3-1278-5a47bf6ee188; dce_opnum:31; dce_stub_data; pcre:"/^(\x00\x00\x00\x00|.{4}(\x00\x00\x00\x00|.{12}))/s"; byte_jump:4,-4,multiplier 2,relative,align,dce; byte_test:4,>,256,0,relative,dce; metadata:policy balanced-ips drop, policy connectivity-ips drop, policy max-detect-ips drop, policy security-ips drop, service netbios-ssn; reference:bugtraq,19409; reference:cve,2006-3439; reference:url,technet.microsoft.com/en-us/security/bulletin/MS06-040; classtype:attempted-admin; sid:7209; rev:20;)[18]

[18] **SNORT, [online] Disponible en internet, agosto 2016 <URL:www.snort.org>**

9. EVALUACIÓN DEL DISEÑO

Para evaluar el diseño presentado se montó un laboratorio, el cual consta de cuatro máquinas virtuales las cuales representan varios roles que se encontrarían en la compañía, estas estarán interconectadas entre sí, sobre el mismo segmento de red como se observa en la figura 16 y cuadro 10.

Figura 16. Estructura laboratorio.



Fuente: Autor

Cuadro 10. Máquinas virtuales

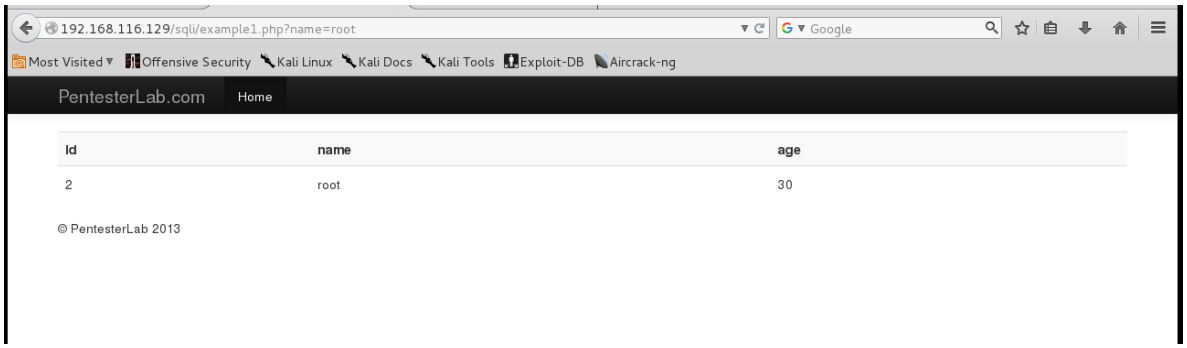
Ip´s	Máquina virtual
192.168.116.129	Servidor web
192.168.116.128	Snort
192.168.116.130	Kali
192.168.116.131	Windows

Fuente: Autor

9.1 PRUEBA SQL INJECTION

Se configura el servidor web con una edición de web for pentester como se observa en la figura 17.

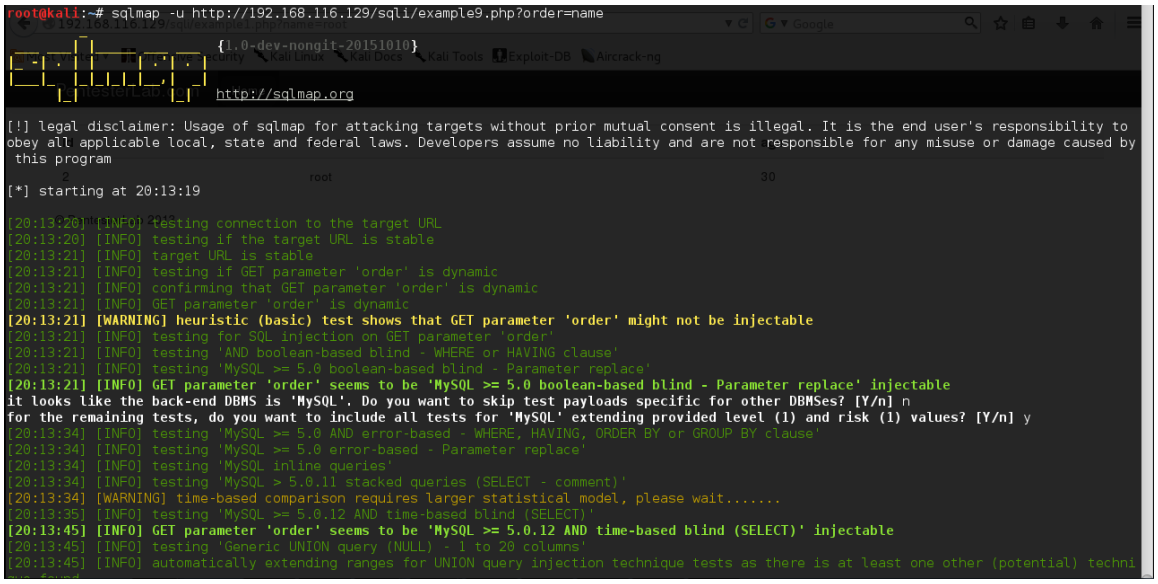
Figura 17. Imagen servidor web



Fuente: Autor

Se realiza un ataque de SQL injection al servidor web, específicamente sobre la url http://192.168.116.129/SQLi/example1.php?name=root con la herramienta SQLmap, como se observa en la figura 18.

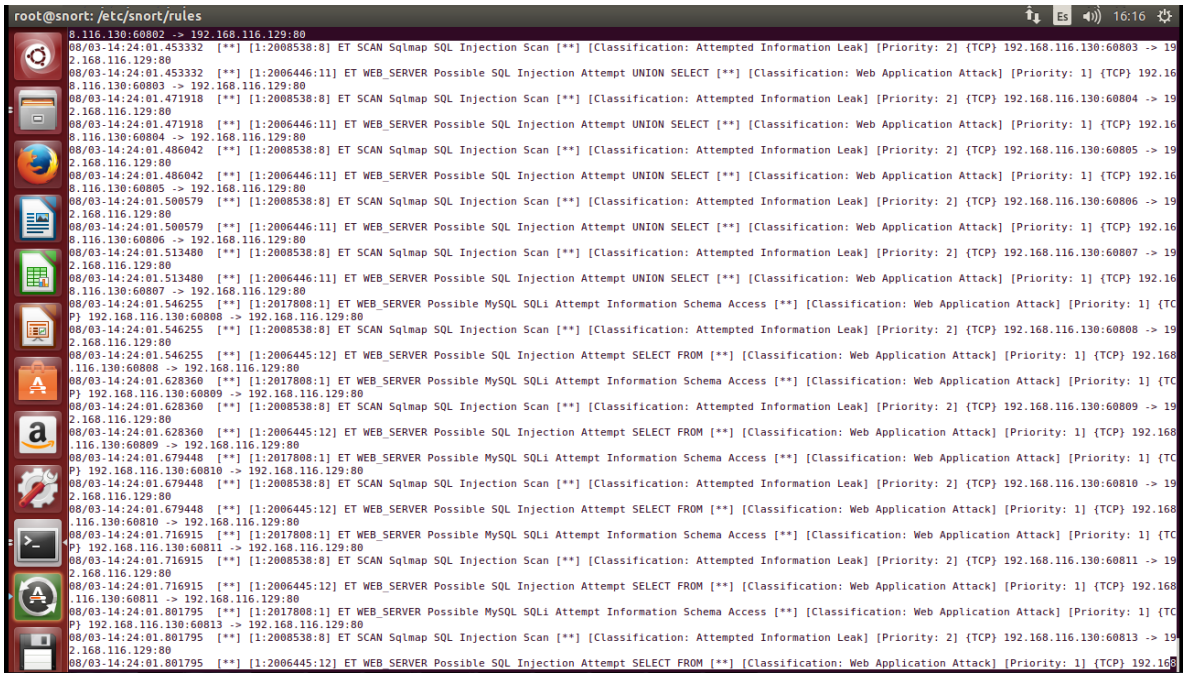
Figura 18. Ataque SQL injection con SQLmap al servidor web.



Fuente: Autor

Se observa que el IDS detecta el ataque y empieza a generar las alarmas como se observa en la figura 19. Cuando snort genera un mensaje de alerta, este usualmente muestra los siguiente [**] [116:56:1] (snort_decoder): T/TCP Detected [**] el primer número es el id del generador, este le dice al usuario que componente de snort genero la alarma. El Segundo número es el snort ID (a veces conocido como ID Firma). SID basados en reglas se escriben directamente en las reglas con la opción SID. El tercer número es el id de revisión, este número se usa principalmente cuando se escribe firmas, ya que cada versión de la regla debería incrementar este número con la opción rev.

Figura 19. Detección de ataque SQL injection.

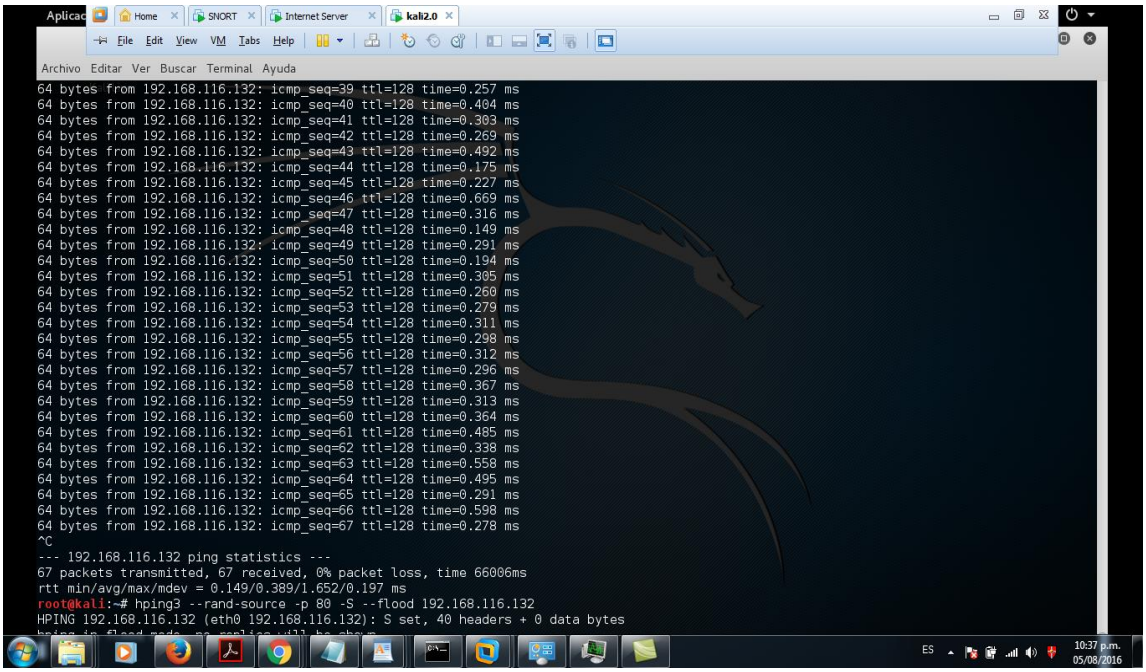


Fuente: Autor

9.2 PRUEBAS CON ATAQUE DoS (Denegación de servicio)

Se realiza un ataque de denegación de servicio con la herramienta hping3 al servidor con Windows server 2003 el cual representa el servidor de controlador de dominio de SilverIT, el ataque es lanzado desde la maquina kali, como se ve en la figura 20.

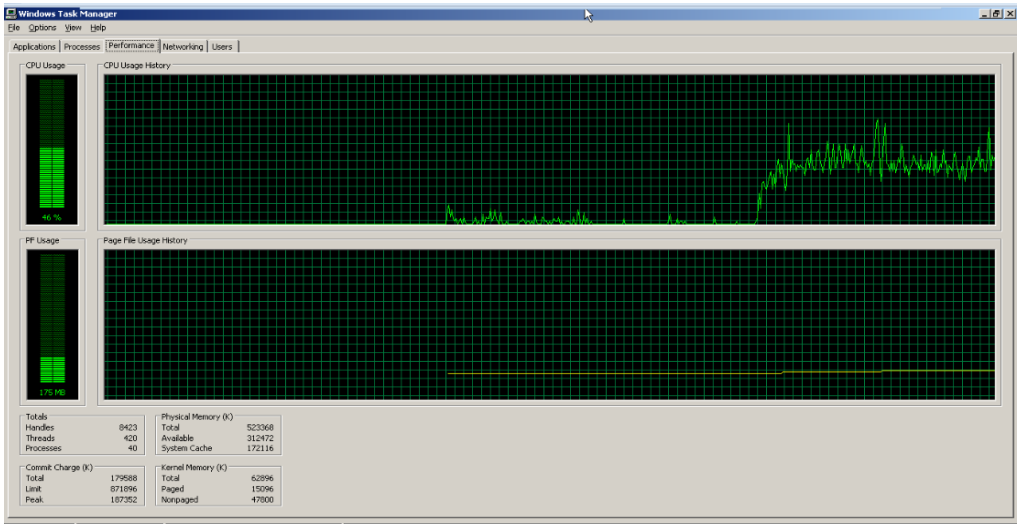
Figura 20. Ataque denegación de servicio con hping3



Fuente: Autor

El servidor con Windows server aumenta significativamente el uso de la cpu afectando su desempeño como se observa en la figura 21.

Figura 21. Incremento en procesamiento por ataque de DoS

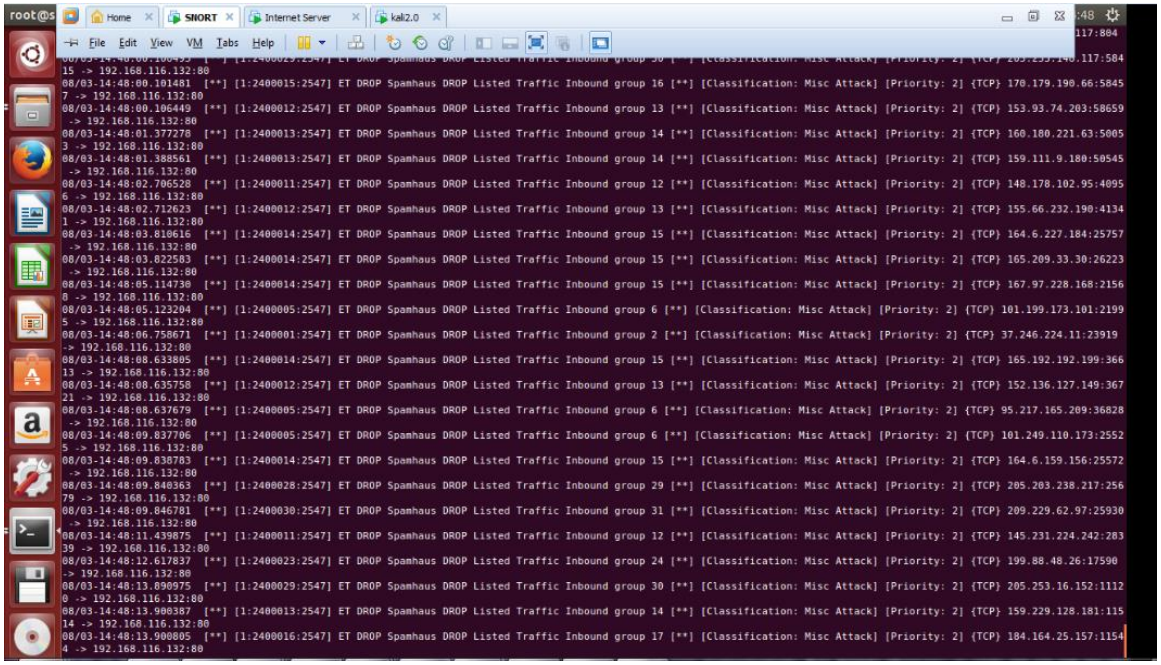


Fuente: Autor

Snort detecta el ataque de denegación de servicio lanzado hacia el servidor, ve muchas peticiones hacia el servidor desde diferentes direcciones ip como se ve en

la figura 22.

Figura 22. Detección ataque denegación de servicio.

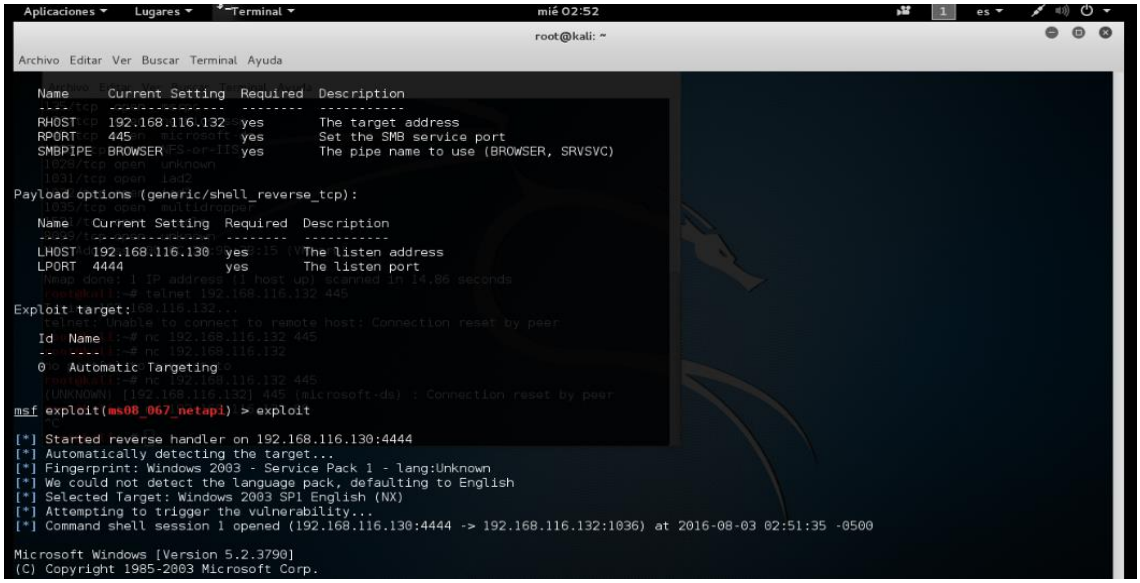


Fuente: Autor

9.3 PRUEBAS CON EXPLOIT MS08_067_NETAPI

Para este ataque se hizo uso de la herramienta metasploit, se utilizó el exploit **ms08_067_netapi** con el payload **generic/shell_reverse_tcp**, se ataca el servidor con windows server, el ataque es exitoso como se observa en la figura 23.

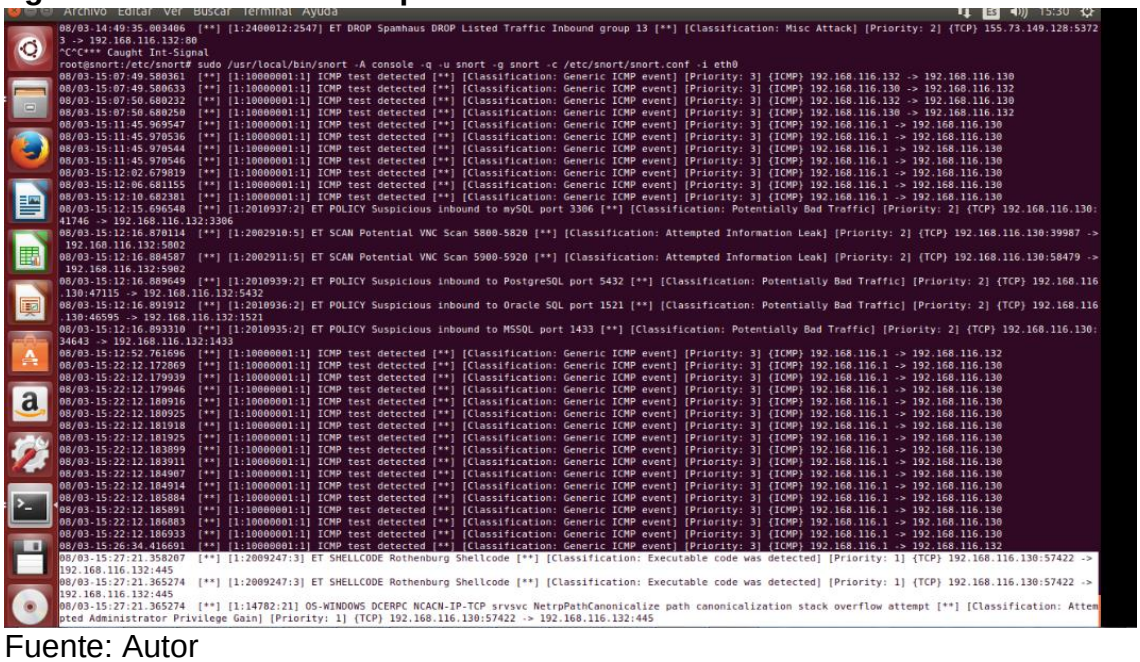
Figura 23. Ataque Con Metasploit



Fuente: Autor

Snort detecta el ataque indicando que un código fue ejecutado y que gano acceso al servidor como administrador, como se observa en la figura 24.

figura 24. Detección de exploit



Fuente: Autor

10. CONCLUSIONES

- SilverIT S.A.S redujo el nivel de riesgo sobre sus activos de información, ya que ahora puede detectar ataques tempranamente y asi tomar acciones reactivas en poco tiempo.

- Se pudo comprobar la eficacia del detector de intrusos con varios ataques generados bajo un ambiente controlado, lo cual permite deducir que el diseño realizado ha sido exitoso.

- Con el tiempo es posible aumentar el número de firmas con el fin de cubrir otros vectores de ataque.

- Snort es un IDS muy popular por ser de código abierto, tener soporte, creación de firmas nuevas constantemente y tener el apoyo de una comunidad completa.

- Los detectores de intrusos deben ser complementarios y complementados con otro tipo de controles para asegurar un mayor nivel de seguridad en la red (Defense in depth).

BIBLIOGRAFÍA

- INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Referencias documentales para fuentes de información electrónicas. NTC 4490, Bogotá D.C 1998.

- INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Documentación Presentación de tesis, trabajos de grado y otros trabajos de investigación. NTC 1486, Bogotá D.C 2008.

- INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Referencias bibliográficas contenido, forma y estructura. NTC 5613, Bogotá D.C 2008.

- NATIONAL INSTITUTE OF STANDARS AND TECHNOLOGY, Guide to intrusión detection and prevention systems (IDPS). SP 800-94, Gaithersburg 2007 2-4 p.

- Oates, Briony. Researching Information Systems and computing. Thousand Oaks, california 91320, SGE publications inc, 2006. 111 p.

- Tsai, Jeffrey J. P. Intrusion Detection: A Machine Learning Approach. River Edge, NJ, USA: World Scientific & Imperial College Press, 2011. ProQuest ebrary. Web. 24 September 2015. 41 p.

- Beale, Jay, et al. Snort 2.0 Instrusion Detection, Rockland, MA, Syngress Publishing, 2003. 1-100 p.

- GONZALEZ GOMEZ, DIEGO. Sistemas de Detección de Intrusiones. Barcelona. 2003. 17-18 p.

- Mira Alfaro José Emilio. Implantación de un sistema de detección de intrusos en la universidad de valencia. Valencia, España. Universidad de valencia. Facultad de informática. 13 p.

- Galindo Jimenez Carlos. Diseño y Optimizacion de un sistema de detección de intrusos hibrido. Almeria, España. Universidad de Almeria. Facultad de informática 40-42 p.

- Ec council CEHv8 Module 14 SQL Injection [Diapositivas], 2014.

- Andrews, Brett et al. 2016 Trustwave Global Security report, Trustwave holdings, chicago 2016. 20 p.

- **SNORT users manual, [online] Disponible en internet, agosto 2016. <URL:https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/100/original/snort_manual.pdf?AWSAccessKeyId=AKIAIXACIED2SPMSC7GA&Expires=1471902383&Signature=2maclYPE56v2%2B6NUGoKGBvRn%2B7U%3D>.**

- **SNORT setup guide, [online] Disponible en internet, agosto 2016. <URL:https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/090/original/Snort_2.9.8.x_on_Ubuntu_12-14-15.pdf?AWSAccessKeyId=AKIAIXACIED2SPMSC7GA&Expires=1471903229&Signature=CEgCbj0IDMj8JqwirzOOZXT9bic%3D>.**

- **Wikipedia, sistema detección de intrusos, [online] Disponible en internet, julio 2015. <URL:https://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos>.**

- **ESET, ataques remotos, [online] Disponible en internet, agosto 2016. <URL:http://soporte.eset-la.com/kb2907/?locale=es_ES>.**

GLOSARIO

ARP SPOOFING: el principio del ARP Spoofing es enviar mensajes ARP falsos (falsificados, o spoofed) a la Ethernet. Normalmente la finalidad es asociar ladirección MAC del atacante con la dirección IP de otro nodo (el nodo atacado), como por ejemplo la puerta de enlace predeterminada (gateway).[19]

CRACKER: el término cracker (del inglés cracker, y este de to crack, 'romper', 'quebrar') se utiliza para referirse a las personas que "rompen" algún sistema de seguridad. Los crackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por el desafío.[20]

DEFENSE IN DEPTH: el principio de defensa en profundidad es que los mecanismos de seguridad en capas aumentan la seguridad del sistema en su conjunto.[21]

DNS: abreviatura del inglés que significa servicio de nombres de dominio, permite controlar la configuración de correo electrónico y sitio web de tu nombre de dominio. Cuando los visitantes van a tu nombre de dominio, la configuración de DNS controla a cuál servidor de la empresa se dirigen.[22]

EXABYTES: un exabyte es una unidad de medida de almacenamiento de Datos cuyo símbolo es el 'EB'. Equivale a 10^{18} bytes.[23]

EXPLOIT: es un programa o código que se aprovecha de un agujero de seguridad (vulnerabilidad) en una aplicación o sistema, de forma que un atacante podría usarla en su beneficio.[24]

FTP: (protocolo de Transferencia de Archivos) en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.[25]

GLP: la licencia pública general de GNU o más conocida por su nombre en inglés GNU General Public License (o simplemente sus siglas del inglés GNU GPL) es la licencia más ampliamente usada en el mundo del software y garantiza

---

[19] Wikipedia, [online] Disponible en internet, septiembre 2016 <url: https://es.wikipedia.org/wiki/ARP_Spoofing>.

[20] Wikipedia, [online] Disponible en internet, septiembre 2016 <url:https://es.wikipedia.org/wiki/Cracker>.

[21] Owasp, [online] Disponible en internet, septiembre 2016 <url:https://www.owasp.org/index.php/Defense_in_depth>.

[22] Godaddy, [online] Disponible en internet, septiembre 2016 <url: https://es.godaddy.com/help/que-es-el-dns-665>.

[23] Wikipedia, [online] Disponible en internet, septiembre 2016 <url:https://es.wikipedia.org/wiki/Exabyte>.

[24] Welivesecurity, [online] Disponible en internet, septiembre 2016 <url:http://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/>.

[25] RFC, [online] Disponible en internet, septiembre 2016 <url:https://www.ietf.org/**rfc**/**rfc**959.txt>.

a los usuarios finales (personas, organizaciones, compañías) la libertad de usar, estudiar, compartir (copiar) y modificar el software.[26]

HACKER: un hacker es alguien que descubre las debilidades de un computador o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas.[27]

LAMMER: lamer es un anglicismo propio de la jerga de Internet que hace alusión a una persona falta de habilidades técnicas, sociabilidad o madurez considerada un incompetente en una materia, actividad específica o dentro de una comunidad.[28]

MAC FLOODING: los switches LAN usan tablas que contienen una memoria con direcciones mac llamada CAM, con el fin de direccionar el tráfico a puertos específicos, cada vez que se recibe una solicitud y no está en la tabla se crea una nueva entrada, los switches tienen un límite del almacenamiento de direcciones mac, una vez sobrepasa este límite empieza a trabajar como un hub lo cual permitirá que todo el tráfico sea escuchado.[29]

MAN IN THE MIDDLE: el concepto de un ataque MiTM es muy sencillo. Además, no se limita únicamente al ámbito de la seguridad informática o el mundo online. Este método sólo necesita que el atacante se sitúe entre las dos partes que intentan comunicarse; interceptando los mensajes enviados e imitando al menos a una de ellas.[30]

PROTOCOLO: un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física. [31]

---

[26] Wikipedia, [online] Disponible en internet, septiembre 2016 <url: https://es.wikipedia.org/wiki/GNU_General_Public_License**>.**

[27] Wikipedia, [online] Disponible en internet, septiembre 2016 <url: https://es.wikipedia.org/wiki/Hacker_(seguridad_inform%C3%A1tica)>.

[28] Wikipedia, [online] Disponible en internet, septiembre 2016 <url: https://es.wikipedia.org/wiki/Lamer_(inform%C3%A1tica)>.

[29] CISCO, [online] Disponible en internet, septiembre 2016 <url: http://www.CISCO.com/c/en/us/support/docs/switches/catalyst-6000-series-switches/23563-143.html>.

[30] Karpersky, [online] Disponible en internet, septiembre 2016 <url: https://blog.kaspersky.com.mx/que-es-un-ataque-man-in-the-middle/469/>.

[31] Wikipedia, [online] Disponible en internet, septiembre 2016 <url: https://es.wikipedia.org/wiki/Protocolo_de_comunicaciones>.